CA Process Automation

Guia de Instalação

Release 04.2.00

Entrar em contato com o Suporte técnico

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Alterações na documentação

Foram feitas as seguintes atualizações de documentação desde a última release desta documentação:

- O que você deseja fazer? (na página 13) - Este tópico existente tem um novo nome e foi reduzido a links para várias tarefas de instalação.
- Introdução aos componentes de um sistema do CA Process Automation (na página 15) - Este novo capítulo descreve cada componente, começando com os necessários para configurar um sistema simples.
  - Um sistema simples do CA Process Automation (na página 15)
  - Um sistema típico do CA Process Automation (na página 17)
  - Um sistema agrupado do CA Process Automation (na página 19)
  - Associações típicas de bancos de dados (na página 20)
- Os tópicos a seguir foram atualizados para refletir que a única versão do JDK a qual o CA Process Automation Release 4.2 oferece suporte é a JDK 1.7. Esse requisito se aplica apenas aos orquestradores. O CA Process Automation oferece suporte a uma versão Java 6 de um JRE (até JRE 1.6.0_45) para agentes.
  - Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30)
  - Pré-requisitos do JDK (na página 76)
  - Considerações sobre o banco de dados ao atualizar do CA IT PAM 2.x para o CA Process Automation Release 4.2.
  - Atualizar para o JDK versão 1.7
  - Atualizar para o CA Process Automation Release 4.2
- Diretrizes para especificar o nome do servidor de banco de dados para o SQL Server (na página 74)" — Este novo tópico explica que você pode hospedar um banco de dados do CA Process Automation em uma instância nomeada do SQL Server.
- Privilégios de proprietário de banco de dados (na página 76) - Este tópico existente foi corrigido para incluir direitos de atuação em modos de exibição.
- Instalar o orquestrador de domínio (na página 96) - Este tópico existente foi atualizado com novas páginas que foram adicionadas ao assistente de instalação para esta release.
- Instalar um agente de forma interativa (na página 174) - Este tópico existente foi atualizado para documentar uma nova caixa de seleção que especifica se o agente deverá usar a comunicação simplificada nas portas padrão da internet (o padrão) ou a comunicação obsoleta na porta 7003.

- Suporte pós-instalação para atualizações do CA EEM (na página 166) - Este novo tópico descreve como atualizar um CA Process Automation Release 4.2 existente ao atualizar a versão da release do CA EEM ou gerar novos certificados com tamanhos de chave maiores.
- Exemplo de cenário: configurar a instalação existente para gerar novamente os certificados do CA Process Automation (na página 162) —" Este novo tópico fornece o procedimento de instalação a ser seguido se o administrador do CA EEM gerar novamente certificados com chaves de 2048 ou 4096 bits depois de instalar o CA Process Automation com o CA EEM r12.51.
- Pré-requisitos do balanceador de carga F5 (na página 53) - Esta seção existente foi modificada para adicionar alterações para oferecer suporte à comunicação simplificada e para remover referências ao nó principal. Outras alterações foram feitas para aprimorar a utilização.
- Balanceador de carga NGINX (na página 35) - Esta nova seção documenta como configurar o balanceador de carga NGINX, que oferece suporte à comunicação simplificada. Esse balanceador de carga é uma boa alternativa ao Apache, que oferece suporte somente à comunicação obsoleta.
- Sobre a comunicação do agente (na página 158) - Este novo tópico descreve o novo método de comunicação simplificada.

- Como atualizar o CA Process Automation (na página 142) - Esse novo cenário foi adicionado ao capítulo Atualizando para a release atual.
  - Fazer backups e preparar para a interrupção (na página 143) - Este novo tópico foi derivado da experiência de campo com a atualização de um cliente.
  - Executar os pré-requisitos de atualização (na página 144)
  - Atualizar o orquestrador de domínio (na página 146)
  - Atualizar um orquestrador não agrupado (na página 149)
  - Atualizar um nó de agrupamento (na página 152)
  - Executar tarefas pós-atualização (na página 155) - Este novo tópico inclui orientações que foram obtidas da experiência de campo com a atualização de um cliente.
  - Testar os processos com os orquestradores atualizados (na página 156)
  - Alternar os balanceadores de carga do Apache para o NGINX (na página 157)
  - Atualizar os pools do F5, a definição da iRule e a configuração (na página 157)
  - Configurar os agentes para usarem a comunicação simplificada (na página 158)
  - Testar os processos com a comunicação simplificada (na página 159)
- Exemplos de atualização - Este novo apêndice inclui:
  - Exemplo: Atualizar um orquestrador não agrupado da Release 4.1sp01 para a 4.2 (na página 286) - Este novo tópico fornece capturas de tela específicas desse cenário de atualização.
  - Exemplo: Atualizar qualquer nó do orquestrador de domínio da Release 3.1sp01 para a 4.2 (na página 277) - Este novo tópico fornece capturas de tela específicas desse cenário de atualização.
  - Exemplo: Atualizar outro nó do orquestrador de domínio da Release 3.1sp01 para a 4.2 (na página 283) - Este novo tópico fornece capturas de tela específicas desse cenário de atualização.
- Portas usadas pelo CA Process Automation (na página 223) —" Este novo apêndice lista as portas usadas por cada componente de um sistema típico do CA Process Automation.

Índice

Apêndice F: Exemplos de atualização 277

Capítulo 1: O que você deseja fazer?

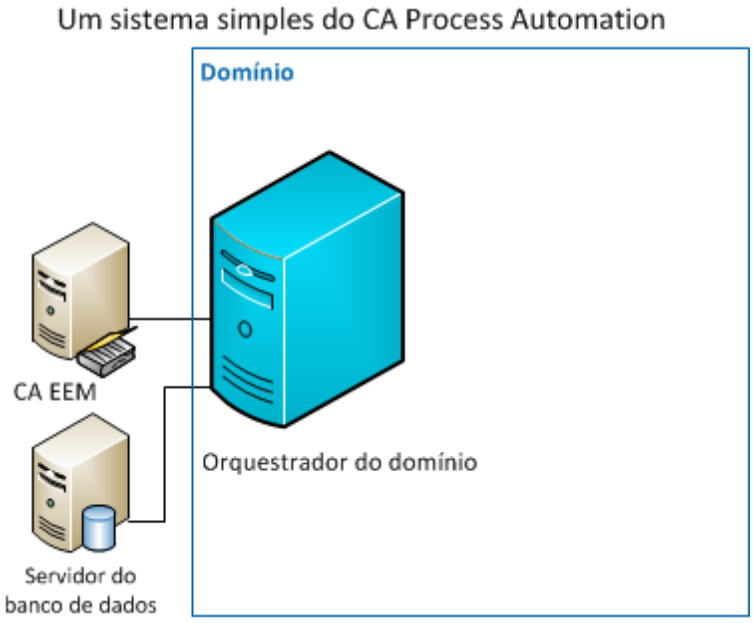
- **Instalar o CA Process Automation pela primeira vez**
  - Introdução aos componentes de um sistema do CA Process Automation (na página 15).
  - Suporte à plataforma e requisitos de hardware (na página 29).
  - Instalar o orquestrador de domínio (na página 65).
- **Atualizar o CA Process Automation a partir de uma release anterior** (na página 141)
- Atualize a release atual do CA Process Automation para:
  - Usar vários domínios do Active Directory. (na página 166) (após atualizar o CA EEM para a versão 12.5)
  - Usar os novos certificados do CA EEM 12.5 (na página 162) (com um CA EEM 12.5 existente)
  - Ativar as comunicações seguras (HTTPS) (na página 170)
  - Usar um novo endereço IP do host (na página 243)
- Instalar um agente (na página 171).
- Criar seu sistema
  - Configurar um balanceador de carga para agrupamento do orquestrador (na página 35)
  - Adicionar um nó ao orquestrador de domínio (na página 185).
  - Instalar um orquestrador adicional (na página 193).
  - Adicionar um nó a um orquestrador adicional (na página 203).
- Solucionar problemas (na página 247)
- Usar o CA SiteMinder com o CA Process Automation (na página 215)

Capítulo 2: Introdução aos componentes de um sistema do CA Process Automation

Esta seção contém os seguintes tópicos:

Um sistema simples do CA Process Automation

Um sistema simples do CA Process Automation inclui três componentes: o orquestrador de domínio, um servidor de banco de dados e o CA Embedded Entitlements Manager (CA EEM).



O orquestrador de domínio

Orquestradores são os servidores do CA Process Automation. Os usuários se conectam a um orquestrador para criar e testar processos, executar processos e configurar o sistema do CA Process Automation de várias maneiras. Todo sistema do CA Process Automation tem um orquestrador de domínio e também pode ter um ou mais orquestradores que não sejam de domínio. Uma implantação simples tem um único orquestrador de domínio.

Um servidor de banco de dados

Durante a instalação do orquestrador de domínio, identifique o servidor de banco de dados no qual criar os três bancos de dados do CA Process Automation.

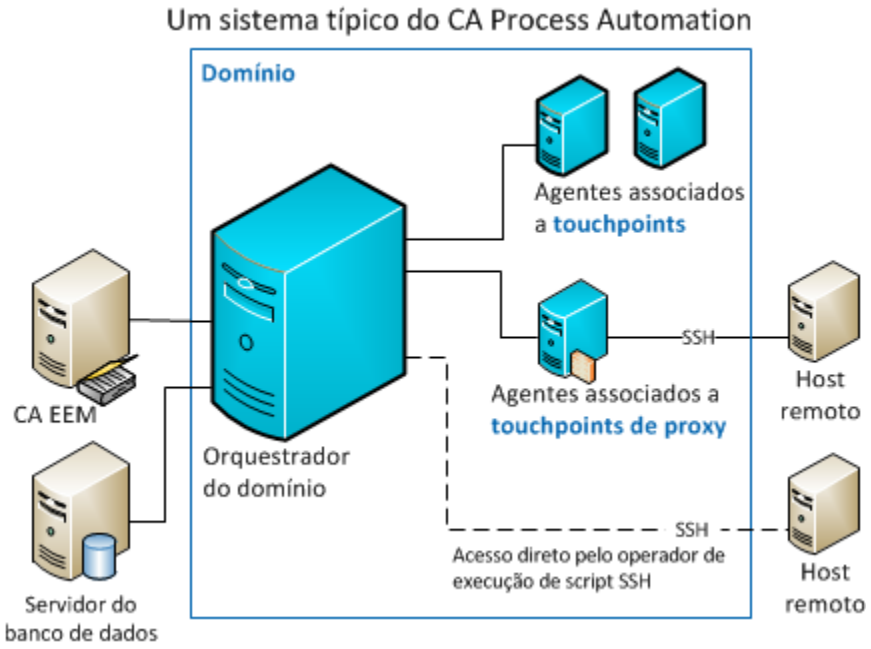
- O banco de dados da biblioteca armazena o conteúdo de automação que você criar. Exemplos incluem os processos, conjuntos de dados e formulários.
- O banco de dados de tempo de execução armazena as informações de estado sobre as instâncias de processo que foram executadas ou que estão sendo executadas.
- O banco de dados de relatórios armazena informações sobre as instâncias de processo que foram executadas em um formato adequado para a execução de relatórios.

CA Embedded Entitlements Manager (CA EEM)

- Durante a instalação do orquestrador de domínio, registre o aplicativo do CA Process Automation no CA EEM. Uma única instância do CA EEM pode ser usada com vários produtos da CA Technologies para fornecer um único local para o gerenciamento de identidades de usuários e suas permissões do aplicativo.
- O CA EEM autentica os usuários do CA Process Automation. O CA EEM tenta corresponder as credenciais que os usuários digitam para efetuar logon com as credenciais de usuários conhecidos do CA Process Automation. Todas as credenciais válidas são definidas diretamente no CA EEM ou, mais comumente, são referenciadas pelo CA EEM a partir de um ou mais repositórios com base em LDAP, como o Microsoft Active Directory.
- O CA EEM também gerencia os níveis de autorização dos usuários do CA Process Automation. No CA EEM, atribui-se permissões para cada conta de usuário depois que o CA Process Automation está instalado para fornecer àquele usuário as permissões relevantes dentro do aplicativo do CA Process Automation.

Um sistema típico do CA Process Automation

Muitas implantações requerem a capacidade de distribuir parte da carga de trabalho para ser executada em hosts diferentes do orquestrador de domínio. Alguns tipos de carga de trabalho podem ser executados em um host remoto sem que um agente esteja instalado nele. No entanto, mais funcionalidade está disponível quando um agente do CA Process Automation está instalado no host de destino.



Agentes

Cada instância do processo consiste em um ou mais operadores. Cada operador é direcionado para ser executado em um host específico, seja direta ou indiretamente, usando o conceito de touchpoints. Cada touchpoint é mapeado para um host específico por meio da configuração do sistema.

O mesmo nome de touchpoint pode mapear para diferentes hosts em diferentes ambientes ou domínios do CA Process Automation. Dessa forma, os touchpoints permitem que o mesmo conteúdo do processo seja implantado de forma inalterada em diferentes ambientes ou domínios do CA Process Automation.

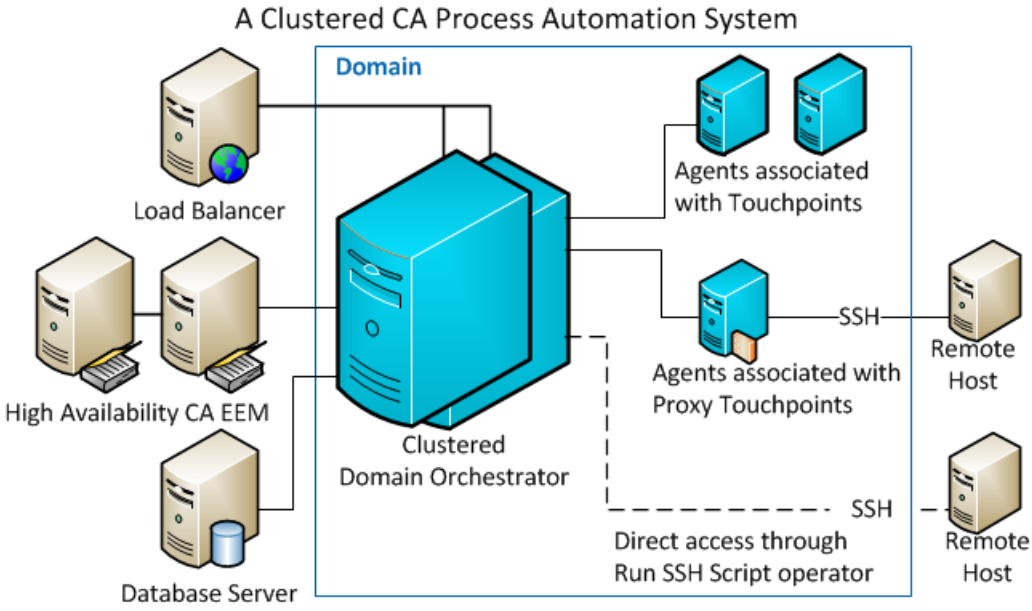
Os touchpoints podem mapear para um orquestrador do CA Process Automation ou para um agente do CA Process Automation. Os touchpoints do proxy mapeiam para um host remoto que não possua nenhum software do CA Process Automation. Os orquestradores podem distribuir a carga de trabalho para um host remoto conectando-se a ele diretamente por meio de SSH ou conectando-se por meio de um agente, que por sua vez, conecta-se ao host remoto por meio de SSH.

Semelhante a um touchpoint, um touchpoint do proxy é uma entidade lógica. Ele é um nome que pode ser usado na criação de processos para especificar um destino de execução do operador. Enquanto um touchpoint é definido e mapeado para um agente específico por meio da configuração do ambiente, um touchpoint do proxy é mapeado para um host remoto sem agente específico. Cada host remoto sem agente (mapeado para um touchpoint do proxy) é gerenciado por um agente instalado em um host diferente. Quando um orquestrador distribui trabalho que está direcionado para um touchpoint do proxy, ele envia o trabalho para o agente que gerencia o host remoto, e esse agente, por sua vez, estabelece uma sessão de SSH com o host remoto para executar o trabalho.

Consequentemente, a tarefa principal de um agente do CA Process Automation é executar a carga de trabalho no host em que está instalado. Além disso, os agentes podem atuar como um gateway por meio do qual a carga de trabalho é distribuída para os hosts remotos em que não é possível instalar um agente.

Um sistema agrupado do CA Process Automation

Muitas instalações implantam um orquestrador de domínio agrupado para alta disponibilidade e escalabilidade da implantação.



Orquestradores agrupados

Um orquestrador agrupado é composto de dois ou mais nós. Em operações normais, a carga de trabalho é compartilhada entre os nós do orquestrador. Outros nós podem ser adicionados para dimensionar a capacidade do orquestrador, conforme necessário. No caso de falha de um nó do orquestrador, os outros nós assumem as responsabilidades do nó com falha até que ele se recupere, fornecendo alta disponibilidade.

Cada nó do orquestrador é instalado em um host diferente. Instale e atualize cada nó separadamente.

Observação: se você já tiver instalado um orquestrador em uma configuração autônoma inicialmente, é necessário executar novamente o assistente de instalação para reconfigurá-lo como um nó de um orquestrador agrupado.

Balanceador de carga

O CA Process Automation oferece suporte a balanceadores de carga de hardware e de software, por exemplo:

- F5
- NGINX
- Apache (com limitações funcionais)

Observação: o balanceador de carga do Apache é suportado para a comunicação entre agentes atualizados e um orquestrador agrupado. No entanto, o balanceador de carga do Apache não oferece suporte ao protocolo que o mecanismo de comunicações simplificadas requer. É possível continuar a usar o modelo de comunicação obsoleta com o Apache, mas se estiver planejando implantar com um balanceador de carga de software, é altamente recomendável que você use o NGINX.

CA EEM de alta disponibilidade

O CA EEM pode ser configurado com um nó de tolerância a falhas para as implantações que exigem uma configuração de alta disponibilidade total.

Opções de configuração avançada

Orquestradores que não são de domínio

É possível particionar a carga de trabalho de automação por meio da implantação de outros orquestradores. Assim como com orquestradores de domínio, esses orquestradores que não são de domínio podem ser agrupados.

Considere o caso em que uma determinada carga de trabalho deve ser direcionada para execução em um centro de dados ou região geográfica específica e o sistema do CA Process Automation precisa ser configurado de forma diferente em cada local. Uma abordagem seria implantar um orquestrador em cada centro de dados e usar a configuração de nível do orquestrador para substituir a configuração de nível do domínio de maneira adequada.

Ambientes

Uma implantação padrão tem um domínio e um único ambiente, o ambiente padrão.

É possível particionar um domínio do CA Process Automation em vários ambientes. Em seguida, vários aspectos da configuração do domínio podem ser adaptados a cada ambiente. Por exemplo, com vários ambientes é possível configurar as coisas de uma forma em um contexto de desenvolvimento de conteúdo e de outra forma em um contexto de teste ou de produção.

Cada ambiente pode ter sua própria biblioteca para que você possa ter potencialmente diferentes versões de conteúdo nos diferentes ambientes.

Os ambientes também particionam a carga de trabalho. Qualquer orquestrador determinado é associado a um ambiente. O ambiente padrão possui o orquestrador de domínio e pode ter um ou mais orquestradores que não são de domínio. Todos os outros ambientes têm um ou mais orquestradores que não são de domínio. Cada orquestrador de domínio e cada orquestrador que não é de domínio pode ser agrupado (vários nós) ou não agrupado (um nó).

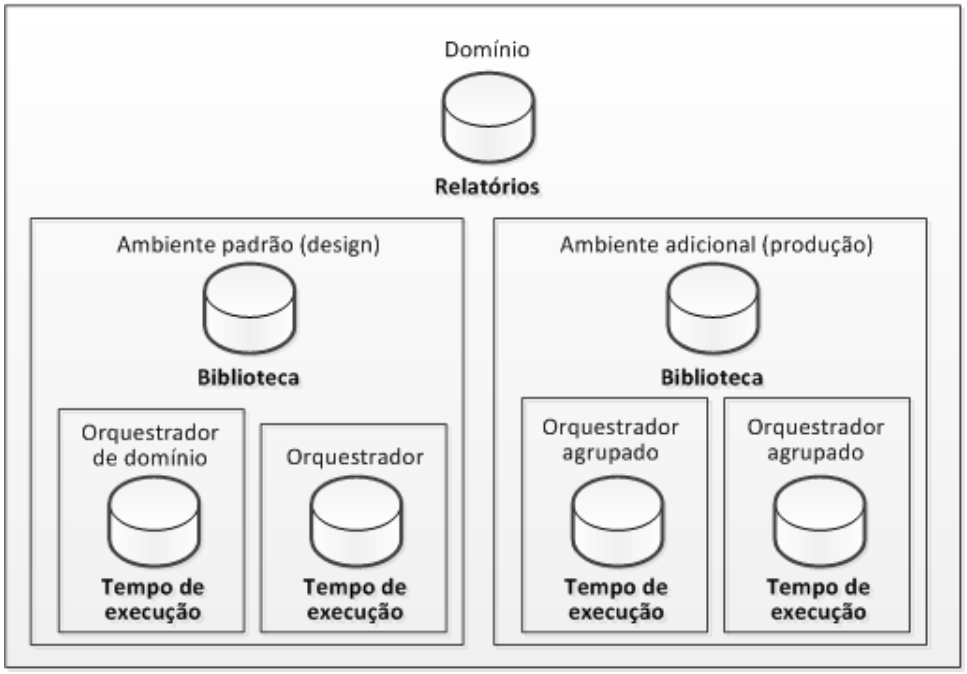
Os ambientes também podem ajudá-lo a particionar a carga de trabalho dentro de um contexto de produção. Por exemplo, um provedor de serviços pode implantar um ambiente por cliente. Essa configuração permite executar o mesmo conteúdo de automação padrão em vários ambientes cuja carga de trabalho é fisicamente particionada. Esses ambientes que estão executando o mesmo conteúdo são configurados de forma diferente e, potencialmente, estão em execução em diferentes localizações geográficas.

Implicações no banco de dados por adicionar ambientes e orquestradores que não são de domínio

Você tem flexibilidade na forma como atribui o compartilhamento de bancos de dados entre os orquestradores. As associações típicas ilustradas são:

- Um banco de dados de relatórios que é compartilhado por todos os orquestradores do domínio. Embora não seja possível compartilhar qualquer banco de dados entre domínios, é possível ter mais de um banco de dados de relatórios.
- Um banco de dados da biblioteca para cada ambiente, onde cada banco de dados da biblioteca é compartilhado por todos os orquestradores no mesmo ambiente.
- Um banco de dados de tempo de execução por orquestrador. Isto é um requisito. Cada orquestrador autônomo (não agrupado) possui seu próprio banco de dados de tempo de execução. Da mesma maneira, cada orquestrador agrupado usa um único banco de dados de tempo de execução.

Associações típicas de bancos de dados



Em uma implantação simples com um orquestrador de domínio não agrupado no ambiente padrão, os três bancos de dados do CA Process Automation são instalados em um servidor de banco de dados.

Adicionar outros ambientes e instalar orquestradores que não sejam de domínio aumenta significativamente a complexidade da configuração do banco de dados necessária.

Mais informações:

Sobre os bancos de dados do CA Process Automation (na página 70)

Exemplo: como os touchpoints ativam a portabilidade do conteúdo

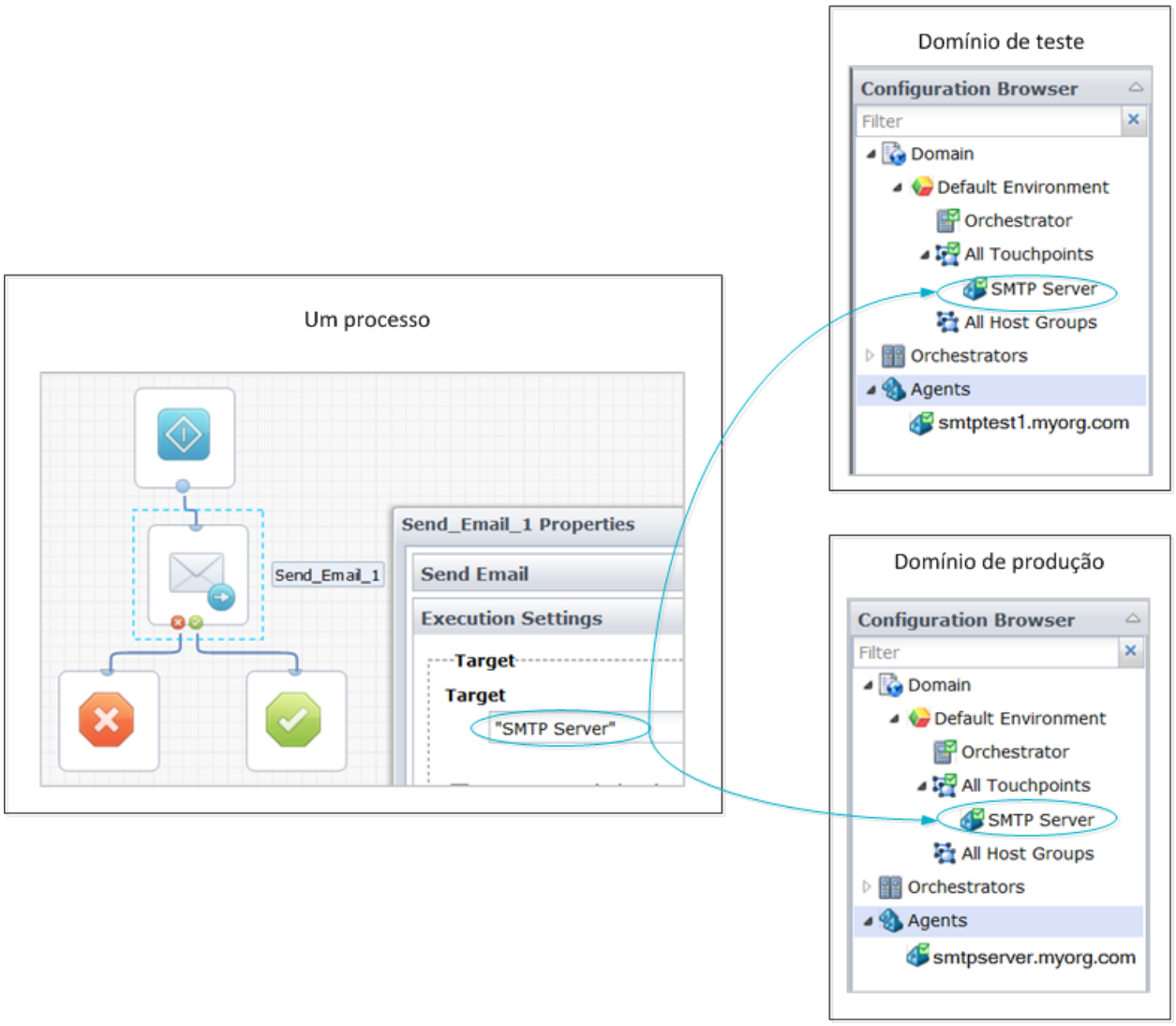
Considere um exemplo de implantação com um domínio de teste e um domínio de produção, cada um com seu próprio servidor SMTP.

- smtptest1.myorg.com no domínio de teste
- smptserver.myorg.com no domínio de produção

O administrador instala um agente em cada servidor SMTP e configura cada agente com o touchpoint nomeado servidor SMTP. Um criador de conteúdo cria um processo com um operador Send_Email, em que o destino da execução está definido para o touchpoint com nome de **servidor SMTP**. Esse processo pode ser implantado sem alterações no domínio de teste e no domínio de produção.

Observação: os guias do CA Process Automation e a ajuda online descrevem como alcançar a portabilidade do conteúdo em ambientes dentro de um único domínio.

Um processo pode ser implantado sem alterações em vários domínios



Como fazer download da biblioteca do CA Process Automation sem acesso à internet

Esta seção descreve como fazer download da biblioteca do CA Process Automation sem acesso à internet.

Observação: para ter acesso à biblioteca do CA Process Automation, é necessário fazer download do arquivo *biblioteca.zip* em todos os nós do CA Process Automation.

Siga estas etapas:

1. Use as credenciais do administrador para efetuar logon em um nó do CA Process Automation com acesso à internet.

   A interface de usuário do CA Process Automation é aberta.

2. Na interface de usuário do CA Process Automation, clique no link Biblioteca a partir do menu suspenso Ajuda, o link Ajuda.

   A biblioteca do CA Process Automation é aberta.

3. Na página da biblioteca do CA Process Automation, clique no link *Fazer download desta biblioteca*.

   Uma caixa de diálogo é exibida solicitando que você salve o arquivo .zip.

4. Crie uma pasta *biblioteca* no seguinte local:

   <*server_loc*>\c2o\.c2orepository\

5. Crie um <*Nome da pasta local*> com base no idioma da biblioteca que estiver selecionado no seguinte local:

   <*server_loc*>\c2o\.c2orepository\biblioteca\

   Observação: com base no idioma da biblioteca que está selecionado, use o devido <*Nome da pasta local*>, como segue:

   - Inglês - <*Nome da pasta local*> está em *en_US*
   - Alemão - *de_DE*
   - Espanhol - es_ES
   - Francês - *fr_FR*
   - Italiano - *it_IT*
   - Japonês - *ja_JP*
   - Português - *pt_BR*
   - Turco - *tr_TR*
   - Chinês - *zh_CN*

6. Descompacte o arquivo .zip e coloque os arquivos da biblioteca do CA Process Automation na pasta local a seguir:

<*server_loc*>\c2o\.c2orepository\biblioteca\<*Nome da pasta local*>\ arquivos da biblioteca.

Agora é possível acessar os arquivos da biblioteca do CA Process Automation a partir da pasta local.

Capítulo 3: Suporte à plataforma e requisitos de hardware

Esta seção contém os seguintes tópicos:

Suporte à plataforma e requisitos para componentes do CA Process Automation

A tabela a seguir resume as plataformas suportadas por componentes do CA Process Automation.

Observação: os sistemas operacionais e os softwares com suporte listados podem mudar ao longo do tempo. Para obter as informações mais recentes sobre o suporte à versão, consulte “Compatibilidades” em support.ca.com.

Componente do CA Process Automation	Sistemas operacionais suportados	Software exigido	Outros requisitos
orquestrador	Microsoft Windows Server 2003 R2 x64 SPx, 2008 x64 SPx, 2012 x64 Solaris SPARC 10 Solaris 11 Red Hat Enterprise Linux 5 x64, 6 x64 SPx CentOS Linux 6 x64	JDK (Java Development Kit - Kit de Desenvolvimento Java) 1.7 **Observação:** o JDK 1.7 também é necessário pela versão 3.4 do Catalyst incorporado. O Catalyst oferece suporte à API REST e a todos os conectores do UCF.	Consulte o tópico Pré-requisitos de instalação do orquestrador de domínio (na página 65).

Componente do CA Process Automation	Sistemas operacionais suportados	Software exigido	Outros requisitos
Agente	Microsoft Windows Server 2003 R2 x64 SPx, 2003 R2 x32 SPx, 2008 x64 SPx, 2012 x64 SUSE Linux Enterprise Server 10 x64,11 x32 SPx, 11 x64 SPx Solaris SPARC 9, 10 Solaris 10 x86 x32 bits, 11 Red Hat Enterprise Linux 5 x64, 6 x32 SPx, 6 x64 SPx CentOS Linux 6 x64 AIX 6.1, 7.1 HP-UX 11i V3 (Itanium)	Uma das seguintes releases do JRE (Java Runtime Environment - Ambiente de Tempo de Execução Java) suportadas pelo sistema operacional. ■ Para Windows, Solaris SPARC e Linux: Oracle JRE 1.6 e 1.7. ■ Para AIX, IBM JRE 1.6 ■ Para HP-UX, o nível mínimo é 1.6_04. HP Java 1.6 (JRE). **Importante:** Não utilize as atualizações de 27 (1.6.0_27) até 29 (1.6.0_29) do Java 6 Runtime Environment. Um problema com essas versões afeta os aplicativos, incluindo o CA Process Automation, que usa o JDBC para se conectar ao Microsoft SQL Server. O banco de dados de bugs SDN lista essa ocorrência como bug 7105007. A atualização 45 do Java 1.6 é a versão mais recente do Java 6 à qual os agentes do CA Process Automation oferecem suporte.	Para touchpoints do proxy e grupos de hosts, cada host remoto deve executar um servidor SSHv2. O host remoto do UNIX deve ter ksh.
Servidor do banco de dados	Consulte a documentação do fornecedor para verificar os sistemas operacionais com suporte.	Um dos seguintes bancos de dados relacionais: ■ MySQL r5.5 ■ Microsoft SQL Server 2005, 2008, 2008 R2, 2012 ■ Oracle 11g R2	Consulte Pré-requisitos do servidor do banco de dados (na página 69) para verificar os requisitos detalhados. Para o Oracle, recomendamos 11.1.0.7 ou 11.2.0.2 ou superior.

Componente do CA Process Automation	Sistemas operacionais suportados	Software exigido	Outros requisitos
Servidor de diretório	Consulte a documentação do CA Embedded Entitlements Manager (CA EEM).	CA Embedded Entitlements Manager (CA EEM) r8.4 SP4 ou CA EEM r12.0 -r12.51.	
Interface de usuário com base em navegador	N/D	Um dos seguintes navegadores: ■ Microsoft Internet Explorer 9x, 10 ■ Google Chrome Release 17, 18 ■ Mozilla Firefox 4.*x* até 15.0 ■ Apple Safari **Observação:** se você utiliza um navegador Firefox ou Chrome, desative o recurso de verificação ortográfica embutido para evitar processamentos desnecessários.	JavaScript ativado Adobe Flash Player

Requisitos de hardware

A tabela a seguir fornece os requisitos mínimos de hardware para cada componente do CA Process Automation:

Componente do CA Process Automation	Hardware exigido
orquestrador	■ Hardware de classe de servidor executando várias CPUs ou CPUs com vários núcleos ■ 8 GB de RAM ■ Espaço livre em disco necessário de 40 GB ■ Conexão de rede de 100 Mbps **Observação:** é recomendável 1.000 Mbps.
Agente	■ Host capaz de executar um sistema operacional com suporte ■ 2 GB de RAM ■ 4 GB de espaço em disco ■ Conexão de rede de 100 Mbps

Componente do CA Process Automation	Hardware exigido
Servidor de banco de dados	Consultar as especificações do fornecedor. Armazenamento adicional, conforme necessário, para os bancos de dados que estão sendo hospedados. **Observação:** é recomendável um mínimo de 40 GB para seus bancos de dados.
CA EEM	Consulte a documentação do CA Embedded Entitlements Manager.
Interface de usuário com base em navegador	Qualquer host capaz de executar um navegador com suporte.

Observação: as configurações podem ser para máquinas físicas e virtuais.

Capítulo 4: Configurar um balanceador de carga para agrupamento do orquestrador

Recomendamos que você substitua os balanceadores de carga do Apache por balanceadores de carga NGINX. O NGINX permite a comunicação simplificada entre os agentes e orquestradores; o Apache oferece suporte somente à comunicação obsoleta.

Se planejar agrupar um orquestrador no futuro, configure um balanceador de carga antes de instalar o orquestrador e, em seguida, configure o orquestrador como node1.

O processo de alto nível do NGINX é semelhante ao do Apache:

1. Instalar um balanceador de carga.
2. Configurar a comunicação básica.
3. Instalar o CA Process Automation, incluindo os nós do agrupamento.
4. Gerar os arquivos de certificado SSL.
5. Configurar a comunicação segura.

Esta seção contém os seguintes tópicos:

Balanceador de carga NGINX

Um *orquestrador agrupado* é um conjunto de nós que são exibidos e que atuam como um único orquestrador, além de usar uma biblioteca compartilhada. Você pode agrupar qualquer orquestrador do CA Process Automation para obter alta disponibilidade, tolerância a falhas e escalabilidade.

Um balanceador de carga, como o servidor HTTP do NGINX, é necessário para o agrupamento de qualquer orquestrador, incluindo o orquestrador de domínio. Um balanceador de carga não faz parte da instalação do CA Process Automation. É necessário instalar e configurar um balanceador de carga antes de instalar o CA Process Automation.

O modo de comunicação simplificado, introduzido no CA Process Automation 4.2, usa soquetes da web e HTTP para produzir uma conexão persistente em uma única via, do agente para o orquestrador. O CA Technologies oferece suporte ao NGINX para este novo método de comunicação simplificada, mas é possível utilizar qualquer balanceador de carga que ofereça suporte a soquetes da web para usá-lo.

Observação: o balanceador de carga do Apache *não* oferece suporte ao modo de comunicação simplificada para agentes, portanto, use o NGINX ou outro balanceador de carga com base em soquete da web para aproveitar esse recurso. Caso não esteja usando o método de comunicação simplificada e desejar usar o método de comunicação obsoleta, é possível instalar o balanceador de carga do Apache.

Instale o balanceador de carga NGINX em um host externo ao CA Process Automation a fim de garantir a compatibilidade com o sistema operacional. Consulte a documentação do NGINX para verificar os sistemas operacionais suportados.

Um balanceador de carga é necessário *apenas* para um orquestrador em uma configuração agrupada e em configurações de SSO (Single Sign On - Logon único) específicas.

Importante: Se você deseja agrupar um orquestrador autônomo, instale e configure um balanceador de carga e, em seguida, reinstale o orquestrador.

Pré-requisitos

Os pré-requisitos para usar o balanceador de carga NGINX são indicados a seguir.

Instalar o NGINX

O NGINX é um software livre de servidor web gratuito que você pode fazer download e instalar para seu sistema operacional. O CA Process Automation foi certificado com o NGINX versão 1.4.2. Use as instruções a seguir para começar.

Windows

Faça download do pacote NGINX e extraia os arquivos.

Linux

Siga estas etapas:

1. Faça download do pacote NGINX e extraia os arquivos.
2. Abra um prompt de comando.
3. Execute o seguinte comando para instalar o NGINX:

```
rpm -ivh nginx-release-rhel-6-0.el6.ngx.noarch.rpm
wget
http://nginx.org/packages/rhel/6/noarch/RPMS/nginx-release-
rhel-6-0.el6.ngx.noarch.rpm
yum install nginx
```

Observação: os comandos anteriores são para o Red Hat Enterprise Linux. Para outras versões do Linux, consulte a documentação do sistema operacional e do NGINX para obter os comandos equivalentes.

Para Windows e Linux, chame o NGINX usando um prompt de comando. Vá até o local do diretório do NGINX e digite:

```
nginx.exe
```

Para verificar se o NGINX foi instalado com êxito e está em execução no momento, acesse o URL em um navegador:

http://*hostname*:80

Copiar os modelos de configuração

Quando o NGINX estiver instalado, extraia os arquivos de modelo da mídia de instalação do CA Process Automation para o diretório de instalação do NGINX.

Siga estas etapas:

1. Navegue até a seguinte pasta na mídia de instalação do CA Process Automation:

   install_dir/DVD1/NginxConfTemplates

2. Extraia os arquivos do NginxConfig.zip.
3. Vá até a subpasta do pam. Esta pasta inclui os seguintes arquivos:

   pam-server.conf

   Usado para configuração não segura.

   secure-pam-server.conf

   Usado para configuração segura.

   pam-rest.conf

   Usado para configuração de REST.

   Esses arquivos são específicos da configuração do CA Process Automation com o NGINX.
4. Copie esses três arquivos e cole-os na seguinte pasta:

   nginx_install_dir/conf

   Agora, é possível configurar o balanceador de carga NGINX.

Comunicação básica

As instruções a seguir descrevem como configurar uma comunicação básica, não segura, para o NGINX nos sistemas Windows e Linux.

Windows

Siga estas etapas:

1. Vá até a seguinte pasta

   `nginx_install_dir/conf`

   Esta pasta contém o arquivo pam-server.conf.

2. Abra o arquivo pam-server.conf.

3. Há três blocos de código que requerem edição em cada nó que seja adicionado.

   a. Adicione o nome do host do node1 no bloco **upstream loadbalancer**:
   `server <Digite o nome de host do node1 aqui>:8080 max_fails=3 fail_timeout=3s`

   b. Adicione o nome do host do node1 no bloco **upstream jettyloadbalancer**.
   `server <Digite o nome de host do node1 aqui>:8080 max_fails=3 fail_timeout=3s`

   c. Adicione o nome do host do node1 no bloco **Define node1**:
   `server <nome do host do computador em que o node1 foi instalado>:<porta do servidor jetty> max_fails=3 fail_timeout=3s`

   Substitua o espaço reservado *Digite o nome de host do node1 aqui* por um valor válido. Não altere os números da porta, a menos que você use uma porta diferente para o nó do CA Process Automation.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para "Server Host" ao instalar o orquestrador de domínio.

   Repita essas etapas para cada nó adicional que você instalar.

4. Salve e feche o arquivo pam-server.conf.

5. Abra o arquivo *nginx_install_dir*/conf/nginx.conf.

6. Adicione a seguinte entrada no bloco http no final do arquivo nginx.conf:

   `include nginx_install_dir/conf/pam-server.conf;`

   Essa entrada vincula o NGINX com as alterações de configuração feitas para o CA Process Automation no arquivo pam-server.conf.

7. Salve e feche o arquivo nginx.conf.

   Importante: Execute o restante dessas etapas *depois* de instalar pelo menos um nó do orquestrador. Consulte o tópico Instalação interativa do orquestrador de domínio (na página 92) ou Instalação autônoma do orquestrador de domínio (na página 118) para obter instruções.

8. Depois de ter instalado pelo menos um nó do orquestrador, abra o arquivo *nginx_install_dir*/conf/nginx.conf.

9. Remova quaisquer blocos de código do servidor, pois eles podem entrar em conflito com o servidor identificado no arquivo pam-server.conf.

   Por exemplo:

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

10. Salve e feche o arquivo nginx.conf.
11. Interrompa o NGINX. Em um prompt de comando, vá até o local do diretório do NGINX e digite:

    `nginx –s stop`

12. Reinicie o NGINX.

    As mudanças entram em vigor.

Linux

Siga estas etapas:

1. Vá até a seguinte pasta

   nginx_install_dir/conf

   Essa pasta contém o arquivo nginx.conf.

2. Abra o arquivo nginx.conf.

3. Forneça o bloco de servidor conforme indicado a seguir para verificar o NGINX autônomo.

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Salve o arquivo e feche-o.

5. Vá até a seguinte pasta

   nginx_install_dir/conf

   Esta pasta contém o arquivo pam-server.conf.

6. Abra o arquivo pam-server.conf.

7. Há três blocos de código que requerem edição em cada nó que seja adicionado.

   a. Adicione o nome do host do node1 no bloco **upstream loadbalancer**:
   `server <Digite o nome de host do node1 aqui>:8080 max_fails=3 fail_timeout=3s`

   b. Adicione o nome do host do node1 no bloco **upstream jettyloadbalancer**.
   `server <Digite o nome de host do node1 aqui>:8080 max_fails=3 fail_timeout=3s`

   c. Adicione o nome do host do node1 no bloco **Define node1**:
   `server <nome do host do computador em que o node1 foi instalado>:<porta do servidor jetty> max_fails=3 fail_timeout=3s`

   Substitua o espaço reservado *Digite o nome de host do node1 aqui* por um valor válido. Não altere os números da porta, a menos que você use uma porta diferente para o nó do CA Process Automation.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.

Repita essas etapas para cada nó adicional que você instalar.

8. Salve e feche o arquivo pam-server.conf.
9. Abra o arquivo nginx.conf.
10. Adicione a seguinte entrada no bloco http no final do arquivo nginx.conf:

    `include` *`nginx_install_dir`*`/conf/pam-server.conf;`

    Essa entrada vincula o NGINX com as alterações de configuração feitas para o CA Process Automation no arquivo pam-server.conf.
11. Remova a entrada seguinte:

    `include` *`nginx_install_dir`*`/nginx/conf.d/*.conf;`
12. Salve e feche o arquivo nginx.conf.

    Importante: Execute o restante dessas etapas *depois* de instalar pelo menos um nó do orquestrador. Consulte o tópico Instalação interativa do orquestrador de domínio (na página 92) ou Instalação autônoma do orquestrador de domínio (na página 118) para obter instruções.
13. Depois de ter instalado pelo menos um nó do orquestrador, abra o arquivo *nginx_install_dir*/conf/nginx.conf.
14. Remova quaisquer blocos de código do servidor, pois eles podem entrar em conflito com o servidor identificado no arquivo pam-server.conf.

    Por exemplo:

    ```
    server {
            listen       80;
            server_name  <LOADBALANCER_HOSTNAME>;
    location / {
                 root   /usr/share/nginx/html;
                  index  index.html index.htm;
           }
    }
    ```
15. Salve e feche o arquivo nginx.conf.
16. Interrompa o NGINX. Em um prompt de comando, vá até o local do diretório do NGINX (nginx-1.42) e digite:

    `nginx –s stop`
17. Reinicie o NGINX.

    As mudanças entram em vigor.

Comunicação segura

As instruções a seguir descrevem como configurar uma comunicação segura para o NGINX nos sistemas Windows e Linux. A comunicação segura difere da básica no ponto em que requer o uso de certificados e arquivos de chave.

Windows

A comunicação segura do NGINX requer certificados SSL (arquivos c2okey2.pem e c2ocert.pem). Certifique-se de gerar esses arquivos (na página 50) antes de começar este procedimento.

Siga estas etapas:

1. Vá até a seguinte pasta:

   `nginx_install_dir/conf`

   Essa pasta contém o arquivo secure-pam-server.conf.

2. Abra o arquivo secure-pam-server.conf.

3. Há três blocos de código que requerem edição em cada nó que seja adicionado. Edite os blocos de acordo com as suas medidas de segurança.

   a. Adicione o nome do host do node1 no bloco **upstream loadbalancer**:
   `server <Digite o nome do host do node1 aqui>:8443 max_fails=3 fail_timeout=3s`

   b. Adicione o nome do host do node1 no bloco **upstream jettyloadbalancer**.
   `server <Digite o nome do host do node1 aqui>:8443 max_fails=3 fail_timeout=3s`

   c. Adicione o nome do host do node1 no bloco **Define node1**:
   `server <nome do host do computador em que o node1 foi instalado>:<porta do servidor jetty> max_fails=3 fail_timeout=3s`

   Substitua o espaço reservado *Digite o nome de host do node1 aqui* por um valor válido. Não altere os números da porta, a menos que você use uma porta diferente para o nó do CA Process Automation.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.

   Repita essas etapas para cada nó adicional que você instalar.

4. Atualize as linhas a seguir, especificando o local dos arquivos c2ocert.pem e c2okey2.pem (no diretório nginx_installed_location\conf).

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   Por exemplo:

   ```
   ssl_certificate      <nginx_install_dir\conf\c2ocert.pem>;
   ```

5. Salve e feche o arquivo secure-pam-server.conf.

6. Abra o arquivo nginx.conf.

7. Adicione a seguinte entrada no bloco http no final do arquivo nginx.conf:
   `include nginx_install_dir/conf/secure-pam-server.conf;`

   Essa entrada vincula o NGINX com as alterações de configuração feitas para o CA Process Automation no arquivo secure-pam-server.conf.

8. Salve e feche o arquivo nginx.conf.

   Importante: Execute o restante dessas etapas *depois* de instalar pelo menos um nó do orquestrador. Consulte o tópico Instalação interativa do orquestrador de domínio (na página 92) ou Instalação autônoma do orquestrador de domínio (na página 118) para obter instruções.

9. Depois de ter instalado pelo menos um nó do orquestrador, abra o arquivo *nginx_install_dir*/conf/nginx.conf.

10. Remova quaisquer blocos de código do servidor, pois eles podem entrar em conflito com o servidor identificado no secure-pam-server.

    Por exemplo:

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

11. Salve e feche o arquivo nginx.conf.

12. Interrompa o NGINX. Em um prompt de comando, vá até o local do diretório do NGINX (nginx-1.42) e digite:

    `nginx –s stop`

13. Reinicie o NGINX.

    As mudanças entram em vigor.

Linux

A comunicação segura do NGINX requer certificados SSL (arquivos c2okey2.pem e c2ocert.pem). Certifique-se de gerar esses arquivos (na página 50) antes de começar este procedimento.

Siga estas etapas:

1. Vá até a seguinte pasta

   nginx_install_dir/conf

   Essa pasta contém o arquivo nginx.conf.

2. Abra o arquivo nginx.conf.

3. Forneça o bloco de servidor conforme indicado a seguir para verificar o NGINX autônomo.

```
server {
        listen       80;
        server_name  <LOADBALANCER_HOSTNAME>;
location / {
             root   /usr/share/nginx/html;
              index  index.html index.htm;
       }
}
```

4. Salve o arquivo e feche-o.

5. Vá até a seguinte pasta:

   nginx_install_dir/conf

   Essa pasta contém o arquivo secure-pam-server.conf.

6. Abra o arquivo secure-pam-server.conf.

7. Há três blocos de código que requerem edição em cada nó que seja adicionado. Edite os blocos de acordo com as suas medidas de segurança.

   a. Adicione o nome do host do node1 no bloco **upstream loadbalancer**:
   `server <Digite o nome do host do node1 aqui>:8443 max_fails=3 fail_timeout=3s`

   b. Adicione o nome do host do node1 no bloco **upstream jettyloadbalancer**.
   `server <Digite o nome do host do node1 aqui>:8443 max_fails=3 fail_timeout=3s`

   c. Adicione o nome do host do node1 no bloco **Define node1**:
   `server <nome do host do computador em que o node1 foi instalado>:<porta do servidor jetty> max_fails=3 fail_timeout=3s`

   Substitua o espaço reservado *Digite o nome de host do node1 aqui* por um valor válido. Não altere os números da porta, a menos que você use uma porta diferente para o nó do CA Process Automation.

Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.

Repita essas etapas para cada nó adicional que você instalar.

8. Atualize as linhas a seguir, especificando o local dos arquivos c2ocert.pem e c2okey2.pem (no diretório nginx_installed_location\conf).

```
ssl_certificate      <certificate_location\c2ocert.pem>;
ssl_certificate_key  <certificate_location\c2okey2.pem>;
```

Por exemplo:

```
ssl_certificate      <nginx_install_dir\conf\c2ocert.pem>;
```

9. Salve e feche o arquivo secure-pam-server.conf.
10. Abra o arquivo nginx.conf.
11. Adicione a seguinte entrada no bloco http no final do arquivo nginx.conf:

    `include nginx_install_dir/conf/pam-server.conf;`

    Essa entrada vincula o NGINX com as alterações de configuração feitas para o CA Process Automation no arquivo secure-pam-server.conf.
12. Remova a entrada seguinte de:

    `include nginx_install_dir/nginx/conf.d/*.conf;`
13. Salve e feche o arquivo nginx.conf.

    Importante: Execute o restante dessas etapas *depois* de instalar pelo menos um nó do orquestrador. Consulte o tópico Instalação interativa do orquestrador de domínio (na página 92) ou Instalação autônoma do orquestrador de domínio (na página 118) para obter instruções.
14. Depois de ter instalado pelo menos um nó do orquestrador, abra o arquivo *nginx_install_dir*/conf/nginx.conf.
15. Remova quaisquer blocos de código do servidor, pois eles podem entrar em conflito com o servidor identificado no arquivo secure-pam-server.conf.

    Por exemplo:

    ```
    server {
            listen       80;
            server_name  <LOADBALANCER_HOSTNAME>;
    location / {
                root   /usr/share/nginx/html;
                 index  index.html index.htm;
           }
    }
    ```
16. Salve e feche o arquivo nginx.conf.
17. Interrompa o NGINX. Em um prompt de comando, vá até o local do diretório do NGINX (nginx-1.42) e digite:

    `nginx –s stop`
18. Reinicie o NGINX.

    As mudanças entram em vigor.

Configuração do REST

O CA Process Automation fornece a opção de configurar um balanceador de carga NGINX para a API RESTful do Catalyst. As instruções a seguir descrevem como configurar o balanceador de carga NGINX para usar REST para a comunicação básica e segura nos sistemas Windows e Linux.

Comunicação básica

Siga estas etapas:

1. Vá até a seguinte pasta

   nginx_install_dir/conf

   Esta pasta contém o arquivo pam-rest.conf.

2. Abra o arquivo pam-rest.conf.

3. Edite o seguinte bloco de código:

   ```
   HTTP
   upstream ucfcluster  {
     server <Digite o nome do host do node1 aqui>:7000 max_fails=3
   fail_timeout=5s;
     server <Digite o nome do host do node2 aqui>:7000 max_fails=3
   fail_timeout=5s;
   }
   ```

   Substitua o espaço reservado *Digite o nome de host do node1 aqui* por um valor válido. Não altere os números da porta, a menos que você use uma porta diferente para o nó do CA Process Automation.

   Repita essas etapas para cada nó adicional que você instalar.

4. Salve e feche o arquivo pam-rest.conf.

5. Abra o arquivo nginx.conf.

6. Adicione a seguinte entrada no bloco http no final do arquivo nginx.conf:
   `include` *`nginx_install_dir`*`/conf/pam-rest.conf;`

   Essa entrada vincula o NGINX com as alterações de configuração feitas para o CA Process Automation no arquivo pam-rest.conf.

7. Salve e feche o arquivo nginx.conf.

   Importante: Execute o restante dessas etapas *depois* de instalar pelo menos um nó do orquestrador. Consulte o tópico Instalação interativa do orquestrador de domínio (na página 92) ou Instalação autônoma do orquestrador de domínio (na página 118) para obter instruções.

8. Depois de ter instalado pelo menos um nó do orquestrador, abra o arquivo *nginx_install_dir*/conf/nginx.conf.

9. Salve e feche o arquivo nginx.conf.

10. Interrompa o NGINX. Em um prompt de comando, vá até o local do diretório do NGINX (nginx-1.42) e digite:

    `nginx –s stop`

11. Reinicie o NGINX.

    As mudanças entram em vigor.

Comunicação segura

Os arquivos de certificado SSL são necessários para a comunicação segura com REST. Certifique-se de gerar esses arquivos (na página 50) antes de começar este procedimento.

Siga estas etapas:

1. Vá até a seguinte pasta

   nginx_install_dir/conf

   Esta pasta contém o arquivo pam-rest.conf.

2. Abra o arquivo pam-rest.conf.

3. Edite o seguinte bloco de código:

   ```
   ## HTTPS
   upstream sslcluster  {
     server <Digite o nome do host do node1 aqui>:7443 max_fails=3
   fail_timeout=5s;
     server <Digite o nome do host do node2 aqui>:7443 max_fails=3
   fail_timeout=5s;
   }
   ```

   Substitua o espaço reservado *Digite o nome de host do node1 aqui* por um valor válido. Não altere os números da porta, a menos que você use uma porta diferente para o nó do CA Process Automation.

   Repita essas etapas para cada nó adicional que você instalar.

4. Atualize as linhas a seguir, especificando o local dos arquivos c2ocert.pem e c2okey2.pem (no diretório nginx_installed_location\conf).

   ```
   ssl_certificate      <certificate_location\c2ocert.pem>;
   ssl_certificate_key  <certificate_location\c2okey2.pem>;
   ```

   Por exemplo:

   ```
   ssl_certificate      <nginx_install_dir\conf\c2ocert.pem>;
   ```

5. Salve e feche o arquivo pam-rest.conf.

6. Abra o arquivo nginx.conf.

7. Adicione a seguinte entrada no bloco http no final do arquivo nginx.conf:
   `include nginx_install_dir/conf/pam-rest.conf;`

   Essa entrada vincula o NGINX com as alterações de configuração feitas para o CA Process Automation no arquivo pam-rest.conf.

8. Salve e feche o arquivo nginx.conf.

   Importante: Execute o restante dessas etapas *depois* de instalar pelo menos um nó do orquestrador. Consulte o tópico Instalação interativa do orquestrador de domínio (na página 92) ou Instalação autônoma do orquestrador de domínio (na página 118) para obter instruções.

9. Depois de ter instalado pelo menos um nó do orquestrador, abra o arquivo *nginx_install_dir*/conf/nginx.conf.

10. Salve e feche o arquivo nginx.conf.

11. Interrompa o NGINX. Em um prompt de comando, vá até o local do diretório do NGINX (nginx-1.42) e digite:

    `nginx –s stop`

12. Reinicie o NGINX.

    As mudanças entram em vigor.

Gerar arquivos de certificado SSL

A geração dos certificados SSL deve ser feita *depois* de instalar o CA Process Automation, mas *antes* de configurar a comunicação segura para o balanceador de carga. Os certificados SSL não são necessários se você deseja usar a comunicação básica, não segura, no balanceador de carga.

Uma vez gerado, o local do arquivo de certificado deve ser identificado quando você definir a configuração do balanceador de carga para a comunicação segura.

Siga estas etapas:

1. Faça download e instale o OpenSSL de um fornecedor.

   Observação: certifique-se de que o host no qual você instala o OpenSSL possui o JDK instalado.

2. Depois de instalar o CA Process Automation em modo de agrupamento (e pelo menos um nó estiver instalado), o assistente de instalação do CA Process Automation irá gerar o arquivo c2okeystore no seguinte local:

   `\server_location\c2o\.config`

   Copie o c2okeystore e cole-o no seguinte diretório:

   `\jdk_location\bin`

   É possível executar os comandos localmente a partir desse local.

3. Use o keytool no JDK para importar o armazenamento de chaves para o formato pksc12, como segue:

   a. Vá para o diretório jdk_location\bin e execute o seguinte comando:

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      O console solicita a senha do armazenamento de chaves de destino.

      Observação: o arquivo OasisConfig.properties contém a senha do armazenamento de chaves. Localize o arquivo nesse diretório: `\server_location\c2o\.config\`

      Abra o arquivo e copie a senha. O valor pode ser encontrado próximo à entrada KEYSTOREID=.

      Por exemplo, KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. A senha é 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Cole a senha no prompt de senha do armazenamento de chaves no console aberto.

   c. Quando solicitado, digite novamente a senha.

   d. No prompt de senha da chave de origem, digite a senha novamente.

      Um arquivo c2okeystore.p12 é gerado no diretório \jdk_location\bin.

   e. É necessário converter o armazenamento de chaves p12 formatado em arquivos de chave e de certificado PEM formatados. Para fazê-lo, execute o comando openssl no local do diretório \jdk_location\bin:

      ```
      openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
      ```

   f. No prompt da senha de importação, digite a senha do armazenamento de chaves.

   g. No prompt da frase secreta do PEM, digite qualquer frase.

h. Digite novamente a frase secreta do PEM.

i. Execute o comando a seguir no local do diretório \jdk_location\bin:
`openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem`

j. No prompt da senha de importação, digite a senha do armazenamento de chaves.

k. No prompt da frase secreta do PEM, digite a frase que você criou anteriormente para a etapa g.

l. Digite novamente a frase secreta do PEM.

m. Execute o comando a seguir no local do diretório \jdk_location\bin:
`openssl rsa -in c2okey.pem -out c2okey2,pem`

n. No prompt da frase secreta do PEM, digite a frase que você criou anteriormente para a etapa g.

o. Digite novamente a frase secreta do PEM.

p. Copie os arquivos c2okey2.pem e c2ocert.pem para o diretório \conf do balanceador de carga.

Observação: faça backup desses arquivos.

Pré-requisitos do balanceador de carga F5

Cada orquestrador agrupado precisa de balanceamento de carga. Se possuir um balanceador de carga F5, você poderá usá-lo para balancear o processamento de solicitações do operador ou solicitações de serviços web entre os nós agrupados do orquestrador de destino.

Antes de instalar o primeiro nó de um orquestrador de domínio agrupado ou de outro orquestrador agrupado, prepare o F5 para executar o balanceamento de carga.

Primeiro, colete as seguintes informações:

- A identidade dos hosts ou servidores virtuais em que os nós do orquestrador serão implantados.
- As credenciais para efetuar logon na interface do F5.

Em seguida, configure os seguintes elementos do F5 para que eles funcionem com o CA Process Automation.

1. Crie um nó do F5 para cada nó de agrupamento (na página 54).

   No CA Process Automation, um nó é qualquer host ou servidor virtual no qual um nó de agrupamento do orquestrador está instalado (ou poderá ser instalado no futuro).

2. Crie um pool do F5 para cada agrupamento do CA Process Automation (na página 55).

   No CA Process Automation, cada pool inclui nós de agrupamento do orquestrador que pertencerem ao mesmo orquestrador agrupado.

3. Crie uma iRule do F5 para o CA Process Automation (na página 56).

   No CA Process Automation, uma iRule encaminha solicitações de operadores que usam como destino o touchpoint de um orquestrador agrupado.

4. Crie um servidor virtual do F5 para o CA Process Automation (na página 59).

   F5 pode ter vários servidores virtuais. O CA Process Automation está configurado como um dos servidores virtuais.

5. Configurar o F5 para usar a comunicação simplificada com HTTPS (na página 61).
6. Prepare o balanceador de carga F5 para verificação de comunicação (na página 63).
7. Ative as sessões de aderência no balanceador de carga F5. Sessões de aderência devem estar ativadas no F5 para que ele funciona com um agrupamento do CA Process Automation.

Criar um nó do F5 para cada nó de agrupamento

Em vez de configurar nós de agrupamento quando estiverem presentes no CA Process Automation, você pode configurar os nós que espera adicionar a qualquer orquestrador agrupado desde o início.

Siga estas etapas:

1. Efetue logon no F5.
2. Selecione a guia Principal, clique em Tráfego local e, em seguida, clique em Nós.

   A lista de nós exibe os detalhes a seguir para cada nó da rede que foi definido para o F5: o status, o endereço IP, a partição e o nome do host.
3. Clique em Criar.

   A página Novo nó será exibida.
4. Preencha a seção Propriedades gerais.

   Endereço

   Especifica o endereço IP do novo nó.

   Nome

   Especifica o nome do host do endereço IP associado.
5. Preencha a seção Configuração.

   Monitores de integridade

   Especifica o monitor de integridade para este nó. Se não estiver configurado, selecione Nenhum.

   Padrão: padrão de nó

   Índice

   Especifica um valor ponderado para atribuir ao nó. Se os nós que pertencerem ao mesmo agrupamento tiverem a mesma capacidade, digite 1 como o valor de Índice para cada nó.

   Limite de conexão

   Especifica o número máximo de conexões que o nó pode aceitar.
6. Clique em Finalizado.

   O nó adicionado será exibido na lista de nós.

Criar dois pools do F5 para cada agrupamento do CA Process Automation

Criar dois pools do F5 para cada agrupamento do CA Process Automation. Para cada pool do F5 que você criar, adicione os nós que pertencem ao agrupamento associado.

Por exemplo, crie dois pools como nos seguintes exemplos:

- PAMPOOL chamado PAMSRVPOOL, em que os integrantes usam a porta 8080 (básica) ou a porta 8443 (segura). Esse pool é usado para todas as comunicações
- PAMWSPOOL PAMJETTYPOOL, em que os integrantes usam a porta 80 (básica) ou a porta 443 (segura). Esse pool oferece suporte a agentes configurados para a comunicação simplificada, que usa soquetes da web.

Siga estas etapas:

1. Efetue logon no F5.
2. Selecione a guia Principal, clique em Tráfego local e, em seguida, clique em Pools.

   A lista de pools estará vazia se você estiver configurando pools pela primeira vez. A lista de pools exibe os detalhes a seguir para cada pool: o status, o nome do pool, a partição e o número de integrantes no pool.
3. Clique em Criar.

   A página Novo pool será exibida.
4. Preencha a seção Configuração.
   a. Selecione Básico na lista suspensa.
   b. Digite um nome para o novo pool.
   c. Nos monitores de integridade disponíveis, selecione http e mova-o para a lista ativa.
5. Selecione Round Robin na lista suspensa Método de balanceamento de carga.
6. Selecione Desativado na lista suspensa Ativação de grupo de prioridade.
7. Adicione cada nó ao novo pool do F5 da seguinte maneira:
   a. Selecione a lista de nós, já que você está adicionando um nó já definido.
   b. Selecione o endereço IP (nome do host) na lista suspensa Endereço que identifica o nó a adicionar a esse pool do F5.
   c. Insira um dos seguintes valores para Service Port com base no nível de segurança da comunicação (básica ou segura) e no tipo de comunicação (obsoleta ou simplificada):

      Comunicação obsoleta e básica (não segura)

      8080

      Comunicação simplificada e básica (não segura)

80 (Selecione HTTP, 80 é preenchido automaticamente no campo Service Port).

Comunicação obsoleta e segura

8443

Comunicação simplificada e segura

443 (Selecione HTTPS, 443 é preenchido automaticamente no campo Service Port).

d. Clique em Adicionar.

Os detalhes adicionados para esse nó aparecem na lista de novos integrantes.

8. Clique em Finalizado.

O novo pool é adicionado à lista de pools do F5.

Crie uma iRule do F5 para o CA Process Automation

Uma iRule encaminha solicitações de operadores que usam como destino o touchpoint de um orquestrador agrupado. O F5 cria um URL a partir dessas informações e usa esse URL como o touchpoint de destino. Para criar uma iRule do F5 para o CA Process Automation, copie a definição da iRule fornecida na caixa de texto Descrição. Em seguida, defina os valores para a variável *MyPool*.

Observação: uma iRule é equivalente ao uriworkermap.properties no Apache. Uma iRule identifica um nó de agrupamento do orquestrador para uma solicitação que usa como destino o touchpoint de um orquestrador agrupado. A decisão é tomada com base no URL.

Siga estas etapas:

1. Efetue logon no F5.
2. Selecione a guia Principal, clique em Tráfego local e, em seguida, clique em iRules.

   A lista de iRules estará vazia se você estiver configurando iRules pela primeira vez. A lista de iRules exibe os detalhes a seguir para cada iRule: o nome da iRule e a partição.
3. Clique em Criar.

   A página Nova iRule será exibida.

4. Preencha a seção Propriedades.

   Nome

   Especifica o nome da iRule.

   Definição

   Especifica a definição da iRule. Copie o texto de A definição da iRule (na página 58) nessa caixa de texto.

   Observação: a linguagem de programação usada para iRules é Tcl, ou Tool Command Language.

   Estender a área de texto

   Especifica se é preciso estender a área de texto da caixa de texto Definição para seu tamanho máximo.

   Selecionado - Estende a área de texto para seu tamanho máximo.

   Desmarcado - Apresenta a área de texto em um tamanho menor que o tamanho máximo.

   Quebra de texto

   Especifica se é preciso quebrar o texto para se adaptar à caixa de texto Definição, em vez de exibir uma barra de rolagem horizontal.

   Selecionado - Quebra o texto que ultrapassa a parte visível da caixa de texto Definição, excluindo uma barra de rolagem horizontal.

   Desmarcado - Apresenta o texto como foi digitado, com uma barra de rolagem horizontal, se necessário.

5. Clique em Finalizado.

   A iRule que você adicionar será exibida na lista de iRules.

A definição da iRule

Digite a seguinte definição na caixa de texto Definição para sua nova iRule. Adapte os valores às instruções definidas, conforme necessário.

- Defina a variável BasicPool com valores específicos para o pool atual com a porta como 8080 para a comunicação básica (não segura).
- Defina os endereços IP para NODE1 e NODE2 com valores dos servidores no pool PAMWSPOOL.
- Use set WSPORT "80" para HTTP ou set WSPORT "443" para usar a porta segura (HTTPS) para a comunicação simplificada.

```
when HTTP_REQUEST {
set PAMPOOL "PAMSRVRPOOL"
set PAMWSPOOL "PAMJETTYPOOL"
set NODE1 "10.130.5.146"
set NODE2 "10.130.5.147"
set WSPORT "80"
    switch -glob [HTTP::uri] {
        "/jmx-console*" { pool $PAMPOOL }
        "/web-console*" { pool $PAMPOOL }
        "/c2orepository/*" { pool $PAMPOOL }
        "/c2orepository/oasisHelp*" { pool $PAMPOOL }
        "/c2orepository/htmlFile/aboutUs/*" { pool $PAMPOOL }
        "/c2orepository/htmlFile/language/*" { pool $PAMPOOL }
        "/c2orepository/htmlFile/installation/*" { pool $PAMPOOL }
        "/c2orepository/media*" { pool $PAMPOOL }
        "/c2orepository/thirdParty*" { pool $PAMPOOL }
        "/c2orepository/MainInstallerConfiguration.properties" {
        pool $PAMPOOL }
        "/itpam*" { pool $PAMPOOL }
        "/itpam/ServerConfigurationRequestServlet" { pool $PAMPOOL }
        "/itpam/MirroringRequestProcessor*" { pool $PAMPOOL }
        "/itpam/AgentConfigurationRequestServlet" { pool $PAMPOOL }
        "/itpam/StartAgent*" { pool $PAMPOOL }
        "/itpam/OasisPrimary" { pool $PAMPOOL }
        "/itpam/JNLPRequestProcessor*" { pool $PAMPOOL }
        "/itpam/JNLPRequestProcessor/installation" { pool $PAMPOOL }
        "/itpam/clientproxy/c2oresourceaction" { pool $PAMPOOL }
        "/itpam/clientproxy/c2oreportaction" { pool $PAMPOOL }
        "/mirroringrepository*" { pool $PAMPOOL }
        "/birt/*" { pool $PAMPOOL }
        default { pool $PAMPOOL }
        "/ws/node1" { pool $PAMWSPOOL member $NODE1 $WSPORT }
          "/ws/node1/*" { pool $PAMWSPOOL member $NODE1 $WSPORT }
        "/ws/node2" { pool $PAMWSPOOL member $NODE2 $WSPORT }
          "/ws/node2/*" { pool $PAMWSPOOL member $NODE2 $WSPORT }
        "/*" { pool $PAMWSPOOL }
    }
```

```
}
```

Crie um servidor virtual do F5 para o CA Process Automation

Você pode criar um servidor virtual do F5.

Siga estas etapas:

1. Efetue logon no F5.
2. Selecione a guia Principal, clique em Tráfego local e, em seguida, clique em Servidores virtuais.

   A lista de servidores virtuais exibe os detalhes a seguir para cada servidor virtual: o status, o nome, a partição, o endereço IP de destino, a porta de serviço, o tipo e um link Editar para Recursos.
3. Clique em Criar.

   A página Novo servidor virtual será exibida.
4. Preencha a seção Propriedades gerais.

   Nome

   Especifica o nome do servidor virtual, por exemplo, PAMLB.

   Tipo de destino

   Especifica o host para um único endereço IP.

   Endereço de destino

   Especifica o endereço IP do servidor virtual, por exemplo, 10.130.5.149.

   Porta de serviço

   Especifica a porta associada para o servidor virtual, por exemplo, 80 para HTTP e 443 para HTTPS.

   Estado

   Especifica se o servidor virtual está disponível para balanceamento de carga. Especifique Ativado.

5. Preencha a seção Configuração. Aceite todos os padrões, exceto para Perfil de HTTP.

   Tipo

   Especifica o tipo de servidor virtual. O Padrão é um servidor virtual que direciona todo o tráfego para o pool definido como o pool padrão de balanceamento de carga.

   Padrão: Padrão

   Perfil de HTTP

   Especifica o perfil de HTTP para administrar o tráfego HTTP. Selecione http.

6. Preencha a seção Recursos.

   iRules

   Especifica as iRules a serem ativadas para esse servidor virtual. Selecione o script iRules criado para o orquestrador agrupado.

   Inclua a iRule criada para o pool padrão.

   Pool padrão

   Especifica o nome do pool para o qual o servidor virtual encaminha o tráfego. Especifique o pool do CA Process Automation como o pool padrão.

   Perfil de persistência padrão

   Especifica o perfil de persistência para esse servidor virtual. Por exemplo, source_addr.

   Perfil de persistência de fallback

   Especifica o perfil de persistência que esse servidor virtual usa caso o perfil de persistência padrão não possa ser usado. Por exemplo, dest_addr.

7. Clique em Finalizado.

Configurar o F5 para usar a comunicação simplificada com HTTPS

A comunicação SSL no F5 requer um arquivo de certificado e um arquivo de chave. A comunicação simplificada pode usar somente certificados gerados pela keytool e copiados para o armazenamento de chaves do CA Process Automation.

Siga estas etapas:

1. Gerar arquivos de certificado SSL (na página 50).
2. Fazer upload do certificado SSL e da chave.
   a. Efetue logon no F5.
   b. Clique em Local Traffic, SSL Certificates, Import.
   c. Importe a chave: selecione Key como o tipo de importação, digite o nome da chave, clique em Browse e vá até o local do arquivo de chave e, em seguida, clique em Import.

      user-specified-location/c2okey2.pem

   d. Clique em Local Traffic, SSL Certificates, Import.
   e. Importe o certificado: selecione Certificate como o tipo de importação, digite o nome do certificado, clique em Browse e vá até o local do certificado e, em seguida, clique em Import.

      user-specified-location/c2ocert2.pem

3. Criar o perfil do cliente.
   a. Clique em Local Traffic, Profiles, SSL, Client.
   b. Clique em Criar.
   c. Digite um nome no campo Name. Aceite o padrão para Parent Profile, clientssl.
   d. Selecione Advanced para Configuration.
   e. No lado direito, selecione os campos Certificate, Key e Pass Phrase para torná-los editáveis.
   f. Na lista suspensa Certificate, selecione o certificado c2ocert2.pem importado na etapa anterior.
   g. Na lista suspensa Key, selecione a chave c2okey2.pem importada na etapa anterior.
   h. Nos campos Pass Phrase e Confirm Pass Phrase, digite a frase da chave que foi usada para gerar os arquivos de certificado.
   i. Clique em Finalizado.

4. Criar o perfil do servidor.
    a. Clique em Local Traffic, Profiles, SSL, Server.
    b. Clique em Criar.
    c. Digite um nome no campo Name. Aceite o padrão para Parent Profile, serverssl.
    d. Selecione Advanced para Configuration.
    e. No lado direito, selecione os campos Certificate, Key e Pass Phrase para torná-los editáveis.
    f. Na lista suspensa Certificate, selecione o certificado c2ocert2.pem importado na etapa anterior.
    g. Na lista suspensa Key, selecione a chave c2okey2.pem importada na etapa anterior.
    h. Nos campos Pass Phrase e Confirm Pass Phrase, digite a frase da chave que foi usada para gerar os arquivos de certificado.
    i. Clique em Finalizado.
5. Vincular os perfis de cliente e de servidor ao servidor virtual do F5
    a. Clique em Local Traffic, Virtual Servers, Virtual Server List.
    b. Selecione o servidor virtual para o CA Process Automation, por exemplo, pamlib.

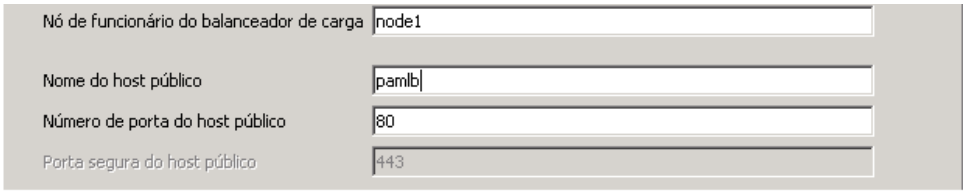
       Observe que Service Port exibe 443 e HTTPS.
    c. Para SSL Profile (Client), selecione clientssl (o padrão usado para o Parent Profile nas últimas duas etapas).
    d. Para SSL Profile (Server), selecione serverssl.
    e. Clique em Finalizado.

Comparação de configurações de porta para HTTPS e HTTP

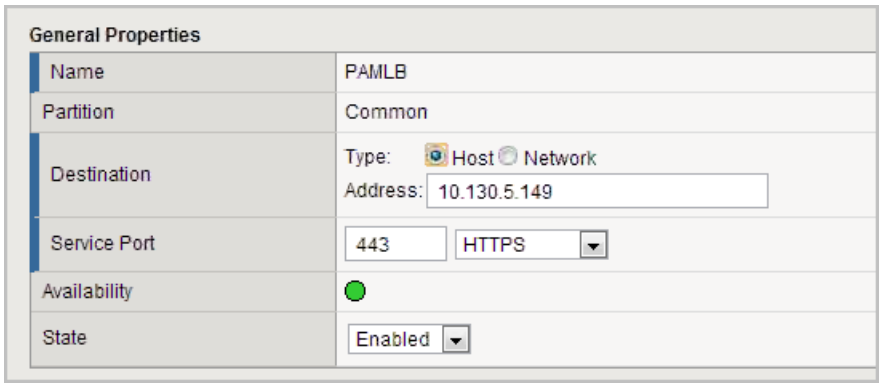
	HTTPS (segura)	**HTTP (básica)**
Porta de serviço	443	80
Integrantes do nó adicionados ao pool	8443	8080
iRule referindo-se à porta do soquete da web	443	80

Preparar o balanceador de carga F5 para verificação de comunicação (Exemplo)

O processo de instalação do orquestrador apresenta uma página de configuração na qual você pode optar por configurar um balanceador de carga:



Em Nome do host público na instalação do CA Process Automation, você digita o nome do host que você definiu no F5. Para verificar se o CA Process Automation pode se comunicar com o host especificado em Nome do host público, o processo de instalação do CA Process Automation envia uma solicitação HTTP Get para o destino que você especificar. O problema do processo de instalação do CA Process Automation é que esse nome do host está mapeado para o endereço IP particular do servidor virtual que o F5 aloca -- um endereço IP que não faz parte de sua rede local do CA Process Automation. No seguinte exemplo, 10.130.5.149 é um endereço IP que faz parte da rede do F5, e não da rede do CA Process Automation.



Sem uma solução alternativa, um erro semelhante ao seguinte ocorre:

```
java.net.UnknownHostException:pamlb
```

Para permitir que a validação de comunicação seja concluída com êxito, crie uma entrada no arquivo de hosts que faça o mapeamento da entrada em Nome do host público para um endereço IP de um servidor que possa responder a essa solicitação.

Por exemplo, crie uma entrada de arquivo de hosts que mapeie a entrada em Nome do host público para o endereço IP de um servidor na rede do CA Process Automation com um balanceador de carga do Apache instalado.

```
xxx.xxx.xxx.xxx      pamlb
```

Depois que o instalador passar da página do balanceador de carga, remova essa linha da solução alternativa do arquivo de hosts.

Observação: como alternativa, é possível configurar o F5 para que o endereço IP alocado possa aceitar a solicitação open http stream do processo de instalação do orquestrador do CA Process Automation. Consulte a documentação do F5 para obter detalhes.

Mais informações:

Portas usadas pelo balanceador de carga (na página 227)

Capítulo 5: Instalar o orquestrador de domínio

O orquestrador de domínio é o que é instalado quando você instala o CA Process Automation pela primeira vez. Antes de instalar o orquestrador de domínio, você deve atender aos pré-requisitos. Você pode instalar o orquestrador de domínio de forma interativa com um assistente. Ou, é possível criar um arquivo de resposta com os valores para os parâmetros que não têm valores padrão e, em seguida, executar o script para instalar o orquestrador de domínio no modo silencioso. Após a instalação, configure as portas e os firewalls. Em seguida, configure o CA Process Automation conforme descrito no *Guia de Administrador de Conteúdo*.

Esta seção contém os seguintes tópicos:

Pré-requisitos para instalação do orquestrador de domínio

Considere configurar um balanceador de carga para a sua primeira instalação para se preparar para a expansão posterior. (A adição de nós de agrupamento pode ser feita quando necessário.)

Observação: é recomendável um balanceador de carga de hardware. Consulte o tópico Pré-requisitos do balanceador de carga F5 (na página 53). Se isso não for possível, recomendamos o NGINX como o balanceador de carga de software de sua escolha. O NGINX para UNIX é altamente escalonável. O NGINX para Windows pode oferecer suporte a até 300 agentes usando a comunicação simplificada. Consulte o tópico Pré-requisitos do balanceador de carga NGINX.

Planeje a instalação inicial do CA Process Automation. Para obter os requisitos do componente, consulte:

- Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30).
- Requisitos de hardware (na página 32).

Siga estas etapas:

1. Identifique um host para o orquestrador de domínio que atenda aos requisitos.

2. Verifique se o host do orquestrador de domínio tem um JDK suportado

   Consulte o tópico Pré-requisitos do JDK (na página 76).

3. Planeje se deseja localizar os componentes de suporte no host com o orquestrador de domínio.

   Consulte o tópico Planejando os locais dos componentes de suporte (na página 67).

4. Identifique o servidor de banco de dados para hospedar os bancos de dados da biblioteca, de relatórios e de tempo de execução para o orquestrador de domínio.

5. Prepare o servidor de banco de dados.

   Consulte o tópico Pré-requisitos do servidor de banco de dados (na página 69).

6. Identifique o host para o CA EEM, caso um CA EEM não esteja sendo usado com outro produto da CA Technologies.

7. Avalie as opções de configuração do CA EEM.

   Consulte Pré-requisitos do CA EEM (na página 78), incluindo Pré-requisitos para configuração da autenticação NTLM.

8. Se o CA EEM estiver configurado com o CA SiteMinder, considere configurar o CA Process Automation para usar o recurso SSO.

   Consulte o tópico Usando o CA SiteMinder com o CA Process Automation (na página 215).

9. Como opção, configure um balanceador de carga se perceber a necessidade de agrupar o orquestrador de domínio posteriormente. Consulte o tópico Configurando um balanceador de carga para agrupamento do orquestrador (na página 35).

10. Grave em um local seguro a senha do certificado que você planeja definir no campo Senha do certificado para o orquestrador de domínio.

    Importante: forneça a mesma senha ao instalar outros orquestradores ou nós adicionais do orquestrador. Se você esquecer a senha, precisará reinstalar cada orquestrador em seu sistema, começando pelo orquestrador de domínio. Essa mesma senha é necessária ao fazer uma atualização para uma nova release.

Planejando os locais dos componentes de suporte

Parte do planejamento de um sistema do CA Process Automation é determinar quais novos componentes você pode colocar no mesmo host com o orquestrador de domínio do CA Process Automation e quais devem ser instalados em hosts separados. Vamos considerar estes componentes de uma rede do CA Process Automation.

- JDK - deve ser colocado
- CA Embedded Entitlements Manager (CA EEM) - pode ser colocado, mas não é recomendável
- Servidores do banco de dados para os bancos de dados do CA Process Automation - podem ser colocados, mas não é recomendável
- Balanceador de carga (se agrupamento for planejado) - não pode ser colocado
- Outros orquestradores - não podem ser colocados
- Nós de agrupamento - não podem ser colocados
- Servidor NTP - externo à rede
- CA SiteMinder (opcional) - pode ser colocado, mas não é recomendável

Cada nó de agrupamento e cada orquestrador geralmente é instalado em um host separado. O servidor NTP pode ser externo à rede.

Para um CA Process Automation com carga mais leve, é possível instalar as seguintes entidades no mesmo host em que você instalou o orquestrador de domínio:

- CA EEM.
- Servidor de banco de dados para os bancos de dados da biblioteca, de relatórios e de tempo de execução.

Considere os seguintes fatores para determinar se é necessário colocar as entidades ou usar vários hosts:

- Características do host

  Os principais fatores incluem a quantidade e a velocidade das CPUs, a memória, o armazenamento em disco e as redes.

- Volume de processos.

  Considere não apenas o número total de processos, mas também as taxas máximas mantidas durante períodos de pico de atividade.

- Implementação de processos.

  Nem todos os processos são iguais. Alguns processos têm poucos operadores, outros têm centenas. Alguns processos contêm muitas atividades de uso intensivo da CPU, ao passo que outros passam a maior parte do tempo aguardando eventos ou interações do usuário. Essa variabilidade dificulta a especificação do carregamento em termos de volume/taxa de processos. Até mesmo na granularidade mais refinada de operadores, a taxa de transferência varia.

- Nível de capacidade de resposta necessário.

  A capacidade de resposta em tempo real nunca é alcançável com a implementação atual. No entanto, até mesmo requisitos menos rigorosos são levados em consideração para verificar quando mais hardware para os orquestradores adicionais deve entrar em ação. Com um SLA (Service Level Agreement - Acordo de Nível de Serviço) rigoroso, o sistema precisa de mais capacidade de reserva para que os períodos de pico ainda tenham um bom desempenho. Sem um SLA, o sistema precisa apenas de capacidade suficiente para cobrir a carga média.

- Intensidade de uso para componentes compartilhados.

  Considere para o que mais o CA EEM e o RDBMS são usados.

Antecipando o crescimento futuro, não é recomendável colocar o CA EEM e o servidor de banco de dados com o orquestrador de domínio. A única forma de determinar se você tem recursos suficientes é realizar um teste de carga completa.

Pré-requisitos do servidor do banco de dados

O CA Process Automation exige que você tenha um ou mais dos seguintes servidores de banco de dados de terceiros nos quais o CA Process Automation possa armazenar e persistir seus dados:

- MySQL Server r5.5
- Microsoft SQL Server 2005, 2008, 2008 R2, 2012
- Banco de dados Oracle 10g Release 2 ou 11g Release 2

O CA Process Automation tem três bancos de dados. Cada um desses bancos de dados pode residir no mesmo servidor de banco de dados, em diferentes servidores de banco de dados do mesmo tipo ou em servidores de bancos de dados de tipos diferentes.

Caso você ainda não possua um desses servidores, consulte os pré-requisitos para cada um antes de obter um. É recomendável que esse servidor e o CA Process Automation residam em hosts separados.

Siga as diretrizes para o tipo de servidor de banco de dados que você estiver usando para a instalação desse orquestrador.

- Preparar o MySQL Server para o CA Process Automation (na página 72).
- Preparar o Microsoft SQL Server para o CA Process Automation (na página 73).
- Preparar o Servidor de dados Oracle para CA Process Automation (na página 75).

Sobre os bancos de dados do CA Process Automation

Cada orquestrador exige três bancos de dados lógicos:

- O banco de dados do repositório, ou o *banco de dados da biblioteca*, é um banco de dados que armazena os objetos de automação criados em pastas na guia Biblioteca do CA Process Automation. Os dados armazenados incluem a estrutura de árvore da biblioteca, a definição completa de cada objeto, bem como a propriedade e as informações de versão.

  Observação: vários orquestradores podem compartilhar o banco de dados do repositório no orquestrador de domínio ou cada orquestrador pode possuir seu próprio.

- O *banco de dados de tempo de execução* é um banco de dados específico do orquestrador que armazena os dados da instância do processo para um único orquestrador ou agrupamento do orquestrador. Os dados incluem informações sobre instâncias do processo em execução no momento, instâncias que foram executadas, mas ainda não foram transferidas para a tabela do arquivo morto e instâncias arquivadas. Você pode acessar os dados atuais e arquivados na guia Operações. Cada registro de tempo de execução inclui o estado, o conjunto de dados e o proprietário da instância do objeto, bem como as informações de programação.

  Observação: cada orquestrador exige um banco de dados de tempo de execução separado. Um orquestrador autônomo possui seu próprio banco de dados. Um agrupamento do orquestrador é visto como um único orquestrador lógico; nesse caso, todos os nós compartilham o mesmo banco de dados.

- O *banco de dados de relatórios* armazena dados históricos das instâncias do processo e do operador. Os administradores podem gerar relatórios quase em tempo real com esses dados usando as definições de relatório predefinido e as definições de relatório personalizado na guia Relatórios.

  Observação: o banco de dados de relatórios é geralmente compartilhado entre todos os orquestradores.

Esses bancos de dados lógicos podem compartilhar um banco de dados físico, mas a prática recomendada é ter bancos de dados separados. O CA Process Automation exige que os nomes dos bancos de dados não diferenciem maiúsculas de minúsculas.

É recomendável um mínimo de 40 GB para os bancos de dados. Operações específicas, como atualizar o CA Process Automation, geram demandas excepcionalmente grandes. Ter um amplo espaço e monitorar periodicamente o consumo de espaço é uma prática recomendada.

Considerações sobre a diretiva de arquivamento

- Os bancos de dados de tempo de execução aumentam à medida que os processos são executados, e o espaço necessário para armazenar esses dados depende do tamanho do conteúdo da instância do processo, bem como das configurações da diretiva de arquivamento do CA Process Automation.
- As instâncias do processo são armazenadas com base na diretiva de arquivamento. É possível configurar a diretiva de limpeza do arquivamento para:
  - Mover instâncias para o arquivo depois de um período de tempo.
  - Excluir automaticamente as instâncias mais antigas sem movê-las para o arquivo morto.
  - Não executar nenhuma ação.

    Observação: quando a diretiva está configurada para não executar nenhuma ação, é recomendável executar as tarefas de arquivamento de dados fora do CA Process Automation.
- A diretiva de arquivamento é específica do orquestrador.

Observação: consulte o tópico Configurar as diretivas do orquestrador no *Guia de Administrador de Conteúdo*.

Mais informações:

Opções de configuração avançada (na página 20)

Preparar o servidor MySQL para o CA Process Automation

Durante a instalação do orquestrador de domínio ou de um orquestrador adicional, o instalador cria bancos de dados do CA Process Automation no MySQL Server especificado. O instalador requer os seguintes requisitos:

- Durante a instalação, vá para o driver do JDBC para MySQL. Esse driver não está incluído na mídia de instalação do CA Process Automation.

  Observação: é recomendável usar o driver do JDBC para MySQL versão 5.1.7 e posterior.

- Credenciais de usuário com privilégios administrativos para criar os bancos de dados da biblioteca, de relatórios e de tempo de execução.
- Duas variáveis do MySQL personalizadas para o CA Process Automation.

Antes de instalar um orquestrador que utiliza o servidor do banco de dados MySQL, prepare o servidor do MySQL para o CA Process Automation.

Siga estas etapas:

1. Baixe o driver do JDBC no site do MySQL. Por exemplo, baixe o MySQL Connector/J 5.1.7.
2. Salve o driver em um local que você possa acessar durante a instalação.
3. Abra o MySQL Workbench e selecione Arquivo de opções em Configuração.
4. Defina a variável para o momento em que uma transação aguarda um bloqueio antes de ser revertida:
   a. Selecione a guia InnoDB.
   b. Role para o grupo Vários.
   c. Selecione innodb_lock_wait_timeout.
   d. Altere o valor padrão, 50, para um valor maior que 60.

      ```
      innodb_lock_wait_timeout = 90
      ```
5. Defina o tamanho máximo do pacote em 33554432 bytes (32 MB) para enviar dados para o servidor do e receber dados dele. O padrão é 1048576.
   a. Selecione a guia Rede.
   b. Localize o grupo Dados/Tamanho da memória.
   c. Selecione max_allowed_packet.
   d. Insira o valor necessário.
6. Clique em Aplicar.

   Uma confirmação das alterações a aplicar ao arquivo de configuração do MySQL é exibida.

Preparar o Microsoft SQL Server para o CA Process Automation

Antes de instalar o orquestrador de domínio do CA Process Automation ou um orquestrador adicional, em que os bancos de dados do CA Process Automation estão localizados no SQL Server, execute as seguintes tarefas:

- Verifique se o SQL Server atende aos requisitos do CA Process Automation (na página 73).
- Compreenda como o driver do JDBC 3.0 é mencionado (na página 74).
- Verifique as diretrizes para especificar o nome do servidor de banco de dados para o SQL Server (na página 74).

Verifique se o SQL Server atende aos requisitos do CA Process Automation

O SQL Server que você preparar para os bancos de dados do CA Process Automation devem atender aos seguintes requisitos:

- O SQL Server deve ser instalado ou configurado com a autenticação de modo misto. Você especifica uma conta com autenticação do SQL Server durante a instalação do orquestrador.
- O instalador do orquestrador exige credenciais de usuário com privilégios de administrador para criar os bancos de dados do CA Process Automation.
- O agrupamento do SQL Server para os bancos de dados do CA Process Automation deve ser SQL_Latin1_General_CP1_CI_AS. Por padrão, o instalador do CA Process Automation cria bancos de dados com esse agrupamento.

Examine o arquivo de configuração do SQL Server para verificar se seu SQL Server atende aos requisitos do CA Process Automation.

Siga estas etapas:

1. Vá até o arquivo ConfigurationFile.ini, que é criado em um caminho semelhante ao seguinte:

   ```
   C:\ Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\ yyyymmdd_hhmmss
   ```

2. Verifique se a configuração do modo de segurança é semelhante à seguinte:

   ```
   ; O padrão é Autenticação do Windows. Use "SQL" para a autenticação de modo misto.

   SECURITYMODE="SQL"
   ```

3. Verifique se a configuração das credenciais de conta do administrador do sistema do SQL é semelhante à seguinte:

   ```
   ; Conta(s) do Windows para provisionar como administradores do
   sistema do SQL Server.
   SQLSYSADMINACCOUNTS=".\Administrator"
   ```

4. Verifique se a configuração do agrupamento é semelhante à seguinte:

   ```
   ; Especifica um agrupamento do Windows ou um agrupamento do SQL para
   usar para o mecanismo de banco de dados.
   SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
   ```

Compreenda como o driver do JTDS JDBC é mencionado

Durante a instalação do orquestrador, o instalador exige o driver do JTDS 1.3 para SQL Server, que está incluído no DVD1. O caminho é:

```
.../DVD1/drivers/jtds-1.3.jar
```

Diretrizes para especificar o nome do servidor de banco de dados para o SQL Server

Ao instalar o orquestrador de domínio ou qualquer orquestrador não agrupado, especifique detalhes para três bancos de dados do CA Process Automation: da biblioteca, de tempo de execução e de relatórios. Se você definir o Tipo de banco de dados como MS SQL, use as seguintes diretrizes para especificar o servidor de banco de dados:

- Se você tiver uma única instância do SQL Server no servidor host, especifique o nome do host do servidor. (Esse nome é a instância padrão.)
- Se você tiver várias instâncias do SQL Server no servidor host, especifique a instância nomeada do SQL Server no formato *nome_do_host**instância_nomeada*.

  Uma instância nomeada do SQL Server é outra cópia do SQL Server em execução no mesmo host. Cada cópia é executada de maneira independente; cada cópia é diferenciada pelo nome da instância. Um servidor de banco de dados pode ter muitas instâncias nomeadas, mas apenas uma instância padrão (sem nome).

Prepare o Servidor de dados Oracle para o CA Process Automation

Antes de instalar o orquestrador de domínio ou um orquestrador adicional, que utiliza o Oracle para hospedar seus bancos de dados internos, uma preparação é necessária.

Siga estas etapas:

1. Crie um usuário com permissões de conexão e recursos.
2. Verifique se o Oracle tem espaço de tabela suficiente para hospedar os seguintes bancos de dados:
   - Banco de dados da biblioteca
   - Banco de dados de tempo de execução
   - Banco de dados de relatórios
3. Crie os bancos de dados da biblioteca, de relatórios e de tempo de execução manualmente.
4. Defina as seguintes configurações:
   - Defina o número máximo de conexões como 100 (ou pelo menos 150 para agrupamento).

     Todas as conexões são executadas através dos orquestradores, mas algumas conexões agrupadas são necessárias para um melhor comportamento.
   - Defina o OLTP (Online Transaction Processing) para facilitar as transações.
5. Compreenda como o driver do Oracle JDBC é mencionado.

   Durante a instalação do orquestrador, o instalador exige o driver do JDBC para Oracle, que está incluído no DVD1. O caminho é:

   ```
   .../DVD1/drivers/ojdbc14.jar
   ```

Observações:

- O particionamento *não* é suportado.

Privilégios do proprietário do banco de dados

Quando você inicia o CA Process Automation pela primeira vez ou ao aplicar um patch, o aplicativo ajusta a estrutura do banco de dados ou do esquema.

Os privilégios mínimos do banco de dados que o CA Process Automation requer são os seguintes:

- O direito de acessar metadados (para determinar a estrutura)
- O direito de CAD (create/alter/drop - criar/alterar/ignorar) direitos DDL para tabelas, índices, exibições, restrições e sequências no banco de dados.
- Direitos de leitura ou gravação em todas as tabelas

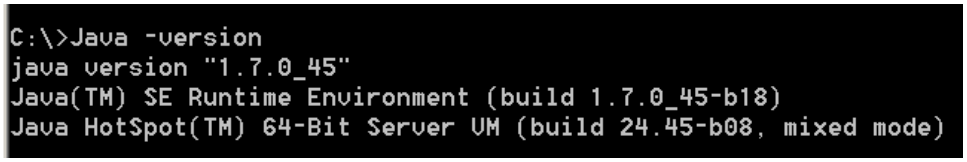
O aplicativo do CA Process Automation requer os seguintes privilégios para as suas tabelas:

- Selecionar
- Inserir
- Excluir

Pré-requisitos do JDK

Antes de instalar qualquer orquestrador, verifique se os pré-requisitos do JDK (Kit de Desenvolvimento Java) foram atendidos. Use o seguinte comando:

```
Java - versão
```



O exemplo anterior mostra uma versão Java válida para o Windows.

Siga estas etapas:

1. Efetue logon no host em que você planeja instalar o orquestrador de domínio.
2. Verifique se o seu Kit de Desenvolvimento Java é Oracle JDK 1.7.

   Observação: para obter detalhes, consulte o tópico Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30). Se a versão padrão do Java for diferente, altere a versão padrão do Java no shell em que você iniciará o instalador do CA Process Automation.
3. Se a versão necessária do JDK não estiver instalada, faça download a partir do site da Oracle e execute o assistente de instalação para instalar o JDK.
4. Para um orquestrador agrupado, certifique-se de que o Oracle JDK está instalado em cada nó.

Definindo o caminho inicial padrão do Java

Se a versão padrão for diferente, altere a versão padrão do Java no shell em que você iniciará a instalação do CA Process Automation.

Siga estas etapas:

1. Procure a pasta DVD1
2. Defina o java padrão no prompt de comando ou shell.

   Windows

   ```
   set JAVA_HOME=<diretório_principal_do_jdk (não_bin)>
   set PATH=%JAVA_HOME%\bin;%PATH%
   ```

   UNIX ou Linux

   ```
   export JAVA_HOME=<diretório_principal_do_jdk (não_bin)>
   export PATH=$JAVA_HOME/bin:$PATH
   ```
3. Inicie o instalador a partir desse prompt de comando ou shell.

   Windows

   ```
   .\ Domain_Installer_windows.bat
   ```

   UNIX ou Linux

   ```
   ./ Domain_Installer_unix.sh
   ```

   O instalador primeiro inicia o instalador de terceiros e, em seguida, inicia o instalador do orquestrador de domínio.

Pré-requisitos do CA EEM

O CA Process Automation usa o CA Embedded Entitlements Manager (CA EEM) para a autenticação e autorização de usuários. O CA EEM é um pré-requisito necessário.

- Se você estiver usando o CA EEM com outro produto da CA Technologies, verifique se é uma versão suportada pelo CA Process Automation. Consulte Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30).
- Se você não tiver o CA EEM ou se o CA EEM for de uma versão mais antiga do que as versões que o CA Process Automation suporta, baixe e instale o CA EEM (na página 79).
- Planejar como autenticar os usuários do CA Process Automation (na página 85).
- Coletar informações relacionadas ao CA EEM para a instalação do orquestrador de domínio (na página 81).
- Para criar duas instâncias do CA EEM na instalação (uma para usar e outra como reserva para a tolerância a falhas), consulte Preparar para a tolerância a falhas para um CA EEM de prontidão (na página 80). Esse procedimento é opcional e pode ser executado posteriormente.

Configurar o CA EEM

O CA Process Automation exige que o CA EEM gerencie a autorização e a autenticação. Uma instância adequada do CA EEM deve estar disponível antes de instalar ou atualizar o CA Process Automation. O CA Process Automation pode usar qualquer versão do CA EEM, da 8.4 SP04 CR10 à 12.5.1, mas alguns recursos do CA EEM que o CA Process Automation pode usar não são suportados em todas as versões do CA EEM. Por exemplo:

O suporte aos certificados de segurança de 2048 e 4096 bits requer o CA EEM versão 12.0 ou posterior.

O suporte a vários domínios do Microsoft Active Directory requer o CA EEM versão 12.5 ou posterior.

Se o seu site contém uma instância do CA EEM que não está na versão necessária, entre em contato com o administrador do site para verificar se a instância do CA EEM pode ser atualizada para o nível desejado. As limitações do suporte à versão de outros produtos que usam a instância do CA EEM podem impossibilitar a atualização da instância.

Nova instalação do CA EEM

Uma nova instalação do CA EEM é necessária se nenhuma instância do CA EEM na versão desejada estiver disponível.

Siga estas etapas:

Faça download de instaladores do CA EEM 12.5.1 a partir do local da mídia de instalação do CA Process Automation.

Siga as instruções fornecidas na documentação do CA EEM ao implantar ou atualizar a instância do CA EEM.

Considerações sobre a configuração do CA EEM

Ao configurar o CA EEM para usar o armazenamento de usuários interno ou um armazenamento de usuários externo, considere as seguintes implicações no CA Process Automation:

Caso selecione o armazenamento de usuários interno padrão, crie contas de usuário para os usuários do CA Process Automation. As credenciais de usuário definidas no CA EEM são usadas para autenticação durante o logon.

Se você apontar para um armazenamento de usuários externos, então, as contas de usuário desse armazenamento são carregadas automaticamente no CA EEM como usuários globais. As credenciais de usuário definidas no Microsoft Active Directory referenciado são usadas para autenticação.

Consulte Referência a usuários globais e grupos globais do Microsoft Active Directory (na página 90). (CA EEM 8.4)

Consulte o tópico Referência a usuários globais de vários Active Directories (na página 90). (CA EEM 12.51)

Ao configurar o CA EEM para o modo FIPS, considere o seguinte:

O CA Process Automation criptografa os dados que são transportados entre o CA Process Automation e o CA EEM.

Se o modo FIPS estiver selecionado no CA EEM, o CA Process Automation deverá ser configurado para usar algoritmos suportados pelo FIPS para a comunicação entre o CA Process Automation e o CA EEM. Durante a instalação do CA Process Automation, selecione a opção Usar o certificado compatível com FIPS para usar algoritmos suportados pelo FIPS.

Preparar para a tolerância a falhas para um CA EEM de prontidão

Considere configurar duas instâncias do CA EEM em uma configuração de alta disponibilidade. Se o CA EEM for configurado dessa maneira, o CA EEM principal funcionará como o servidor de autorização e autenticação de segurança ativo do CA Process Automation. O CA EEM secundário é o servidor de autorização e autenticação de segurança de prontidão. O CA EEM secundário espelha o CA EEM principal. As duas instâncias do CA EEM podem apontar para o mesmo diretório externo.

O CA Process Automation transfere, de maneira automática e transparente, do CA EEM principal para o CA EEM secundário se o CA EEM principal falhar depois que o CA Process Automation fizer a conexão inicial. A tolerância a falhas ocorre mesmo que o servidor principal esteja inativo inicialmente quando você configurar os dois servidores do CA EEM no CA Process Automation.

Consulte a documentação do CA EEM para a versão que está implantada em seu site para obter informações sobre como defini-lo em uma configuração de alta disponibilidade. Informações adicionais estão disponíveis na página de práticas recomendadas de implementação do CA Process Automation (que pode ser acessada por meio de um link rápido na guia Início do CA Process Automation).

Coletar informações relacionadas ao CA EEM para a instalação do orquestrador de domínio

Antes de iniciar a instalação do orquestrador de domínio, tenha em mãos os seguintes detalhes da configuração do CA EEM:

- As credenciais do administrador do CA EEM, onde EiamAdmin é o nome de usuário.
- A versão da release do CA EEM e a configuração do FIPS no CA EEM.

  1. Vá até o CA EEM que você está usando.

     `https://server:5250/spin/eiam`

  2. Selecione o nome do aplicativo do CA Process Automation na lista suspensa Aplicativo.
  3. Digite as credenciais de logon válidas, **EiamAdmin** e a senha associada. Clique em Efetuar logon.
  4. Clique em Sobre. A versão da release do CA EEM e a configuração do FIPS são exibidas em Especificações do produto.

Observação: durante a instalação do CA Process Automation, o processo que registra o aplicativo do CA Process Automation com o CA EEM também gera os certificados que o CA Process Automation usa para se conectar ao CA EEM.

- Se o CA EEM estiver ativado para FIPS, PAM.cer e PAM.key serão gerados.
- Se o CA EEM não for compatível com FIPS, forneça uma senha (a senha do certificado do EEM) antes de registrar o aplicativo do CA Process Automation no CA EEM. Essa senha será usada para proteger o certificado PAM.p12 que é gerado durante o registro do aplicativo do CA Process Automation no CA EEM.
- Se instalar o aplicativo do CA Process Automation no CA EEM *sem registro*, você será solicitado a selecionar o SDK correspondente à versão do seu servidor do CA EEM.

- O nome do host do servidor do CA EEM. Para determinar o nome do host, efetue logon no CA EEM. O nome do host é exibido com o rótulo Back-end na barra de título.

  Importante: a senha de EiamAdmin é necessária para efetuar logon no CA EEM.

- Se você estiver atualizando e planejar configurar o CA EEM para usar vários Microsoft Active Directories, saiba o nome do domínio do AD referenciado no momento. Avalie a possibilidade de especificar esse domínio como o domínio do AD padrão. Os usuários do CA Process Automation que pertencem ao domínio padrão poderão efetuar logon no CA Process Automation com o nome de usuário não qualificado depois de serem reatribuídos a um grupo de aplicativos.
- Registre a senha do certificado que você planeja inserir. Essa senha do certificado controla o acesso às chaves que criptografam senhas e outros dados críticos. A senha do certificado é específica para um único domínio do CA Process Automation. (Essa senha do certificado não está relacionada ao CA EEM, mas é importante registrá-la.)

  Importante: Você deve usar essa mesma senha ao instalar qualquer outro orquestrador ou ao adicionar nós de agrupamento a um orquestrador. Essa mesma senha é uma entrada obrigatória ao atualizar o CA Process Automation.

Identificar a versão do CA EEM SDK que o CA Process Automation utiliza

Você pode determinar se o CA EEM SDK usado pelo CA Process Automation usa o SDK versão 8 ou 12.

Siga estas etapas:

1. Interrompa o orquestrador de domínio.
2. Aumente o nível do log do orquestrador de domínio para INFO.
3. Inicie o orquestrador de domínio.
4. Efetue logon no servidor do CA Process Automation.
5. Verifique os logs.
   - Se o CA Process Automation estiver usando o CA EEM SDK r8.4:

     ```
     13:03:16,859 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByUserName in class:
     com.ca.eiam.SafeGlobalUser. The current EEM SDK's version is
     8
     13:03:16,861 INFO
     [com.optinuity.c2o.eemconfiguration.EEM8Manager]
     (http-user01-m4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM8Manager...
     ```

   - Se o CA Process Automation estiver usando o CA EEM SDK 12.51:

     ```
     13:32:37,195 INFO
     [com.optinuity.c2o.eemconfiguration.EEMManagerFactory]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Found
     method: soRetrieveByPrincipalName in class:
     com.ca.eiam.SafeGlobalUser. The current EEM SDK's version is
     12
     13:32:37,198 INFO
     [com.optinuity.c2o.eemconfiguration.EEM12Manager]
     (http-user02-M4600.ca.com-138.42.24.149-8080-2) Initialized
     EEM12Manager...
     ```

6. Interrompa o orquestrador de domínio, retorne a configuração do nível do log para o nível anterior e, em seguida, reinicie o orquestrador de domínio.

Pré-requisitos para a configuração da autenticação NTLM

Faça o seguinte antes de configurar a autenticação NTLM:

- Verifique se o CA EEM está instalado em um servidor com um sistema operacional Microsoft Windows.
- Verifique se o CA EEM usa o Microsoft Active Directory como o armazenamento de usuários externo.
- Verifique se o CA EEM não está configurado para vários Active Directories ou para uma floresta do Active Directory.
- Verifique se os usuários navegam até o CA Process Automation a partir de um computador com Windows.
- Verifique se o servidor do CA EEM e o computador a partir do qual os usuários navegam até o CA Process Automation fazem parte do mesmo domínio de rede. Se os computadores fizerem parte de domínios aninhados, certifique-se de que o servidor do CA EEM e o computador no qual o aplicativo é iniciado pertençam a domínios que têm um relacionamento de confiança estabelecido.
- Verifique se os usuários do domínio estão incluídos em Grupos de usuários no computador no qual o aplicativo está sendo iniciado.

Planejar como autenticar os usuários do CA Process Automation

Se esta for uma nova instalação do CA Process Automation, parte da preparação é determinar como autenticar usuários do CA Process Automation. A configuração real descrita aqui é realizada após a conclusão da instalação. No entanto, as opções de instalação do CA Process Automation que você selecionar se baseiam nos seus planos. As opções incluem:

- Criar uma conta de usuário para cada usuário do CA Process Automation no CA EEM. O administrador do CA EEM atribui uma ID de usuário para cada conta. Os usuários podem atualizar suas próprias senhas no CA EEM. Quando os usuários efetuam logon no CA Process Automation, o CA EEM autentica os usuários ao verificar se a ID de usuário e a senha (credenciais) digitadas pertencem a uma conta de usuário ativa.
- Referenciar contas de usuário armazenadas em um ou mais Microsoft Active Directories. O CA EEM transmite as credenciais usadas para efetuar logon no CA Process Automation para o AD; o AD executa a autenticação.
- Use a autenticação NTLM (de passagem) sem usar o SiteMinder. O pré-requisito é referenciar as contas de usuário armazenadas em um domínio do AD (Microsoft Active Directory). Não há suporte para a autenticação NTLM se você fizer referência a vários domínios do Microsoft AD. A autenticação NTLM exige que todos os computadores afetados usem um sistema operacional Windows e que estejam no mesmo domínio ou em domínios com relações de confiança.
- Ative o Single Sign On (logon único) usando a autenticação NLTM. Isso é feito por meio do uso do CA SiteMinder ou por atender aos pré-requisitos para configurar a autenticação NTLM (na página 84). Em ambos os casos, selecione a autenticação NTLM durante a instalação. O NTLM manipula a autenticação quando os usuários navegam até o CA Process Automation. Os usuários autenticados têm o logon efetuado com suas credenciais do Windows. Como alternativa, execute a instrução Ativar a autenticação de passagem NTLM após a instalação (na página 130).

Se esta for uma nova instalação do CA Process Automation, parte da preparação é determinar como autenticar os usuários do CA Process Automation. A configuração real descrita aqui é executada após a conclusão da instalação. No entanto, o método de autenticação escolhido determina as configurações especificadas durante a instalação do CA Process Automation. As opções de autenticação são:

Autenticação EEM-based

- Usuário com base em EEM nativo

  Pré-requisitos

  - Instalação do CA EEM

Detalhes: um administrador do CA EEM cria uma conta de usuário no CA EEM para cada usuário que requer acesso ao CA Process Automation. O administrador do CA EEM fornece a cada usuário uma ID de logon. Os usuários podem atualizar suas próprias senhas no CA EEM. Quando os usuários efetuam logon no CA Process Automation, o CA EEM autentica os usuários ao verificar se a ID de usuário e a senha (credenciais) digitadas pertencem a uma conta de usuário ativa.

Ação necessária durante a instalação do CA Process Automation

Nenhuma ação especial necessária

Referência ao diretório LDAP

Pré-requisitos

Instalação do CA EEM

Acesso a um diretório com base em LDAP externo

Detalhes: os seguintes tipos de diretório e configurações estão disponíveis:

AD (Active Directory)

O CA EEM pode ser configurado para fazer referência a contas de usuário armazenadas em um ou mais Microsoft Active Directories. O CA Process Automation transmite ao CA EEM as credenciais de logon e o CA EEM transmite essas credenciais ao AD para validação.

Diretório com base em LDAP que não é do AD

O CA EEM também pode ser configurado para usar um diretório com base em LDAP diferente do AD. A autenticação é manipulada da mesma forma, nesse caso.

Ação necessária durante a instalação do CA Process Automation

Nenhuma ação especial necessária

Single Sign On (logon único) usando a autenticação NTLM

Pré-requisitos

Os mesmos pré-requisitos de quando se usa o AD com a opção do diretório LDAP acima

(NEED TO VERIFY if NTLM authentication is not supported if you reference multiple Microsoft AD domains.)

Além disso, você deve ser capaz de atender aos pré-requisitos para configurar a autenticação NTLM.

Observação: um dos requisitos é que os usuários do PAM executem um sistema operacional Windows e estejam no mesmo domínio, ou em domínios com relacionamentos confiáveis, que o servidor do EEM.

Detalhes: o CA EEM manipula a autenticação por meio de NTLM quando os usuários navegam até o CA Process Automation. Os usuários autenticados têm o logon efetuado com suas credenciais do Windows.

Ação necessária durante a instalação do CA Process Automation

Selecione [NTLM option (not sure of exact term)] na página do assistente do EEM durante a instalação do CA Process Automation. Esta é a maneira recomendada para ativar o SSO.

Observação: é possível ativar a autenticação de passagem NTLM após a instalação, se necessário.

Autenticação SiteMinder-based

Single Sign On (logon único) usando o CA SiteMinder

Pré-requisitos

[Point to SiteMinder doc]

Detalhes: o SiteMinder autentica com um diretório externo e envia o nome do usuário para o CA Process Automation. Em seguida, o usuário é autorizado no CA EEM. [We should probably point the user to the SiteMinder section in our install guide for more details.]

Ação necessária durante a instalação do CA Process Automation

Os cabeçalhos e nome do host do SiteMinder são especificados na página do assistente do balanceamento de carga

Autenticação e autorização de usuários no modo FIPS

O CA EEM pode ser configurado para usar o modo FIPS. Isto é uma opção. Somente se o CA EEM estiver configurado para usar o FIPS, o CA Process Automation poderá ser configurado para usar o FIPS. Mesmo se o CA EEM estiver configurado para usar o FIPS, o CA Process Automation poderá ser configurado para não usar o FIPS.

Esteja o modo FIPS definido como ativado ou desativado, os dados transferidos entre o CA EEM e o CA Process Automation serão criptografados. A diferença está nos algoritmos usados para criptografia.

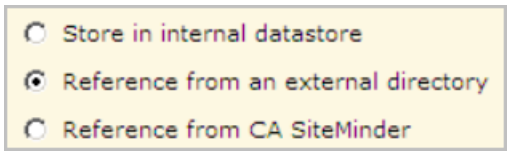
Quando os usuários efetuam logon, o CA Process Automation transfere o nome de usuário e a senha para o CA EEM. O CA EEM retorna os dados de autenticação e autorização para o CA Process Automation.

- Quando o modo FIPS está ativado:
  - Os dados transferidos são criptografados com o algoritmo SHA1 com suporte pelo FIPS.
  - Um certificado PAM.cer é usado.
- Quando o modo FIPS está desativado:
  - Os dados transferidos são criptografados com o algoritmo MD5.
  - Um certificado PAM.p12 é usado.

Definir o tipo de configuração do CA EEM para armazenar usuários globais

Se estiver atendendo aos pré-requisitos do CA EEM para a instalação inicial do CA Process Automation, considere o seguinte:

- Parte da configuração do CA EEM é selecionar se deseja armazenar as credenciais de usuário internamente ou referenciar as credenciais de usuário a partir de um diretório externo ou do SiteMinder.



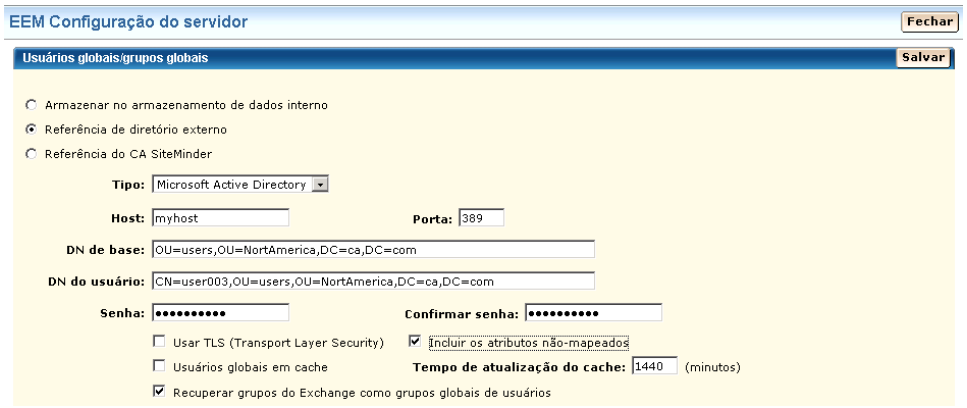
- Se você estiver usando um CA EEM existente que ofereça suporte a aplicativos diferentes do CA Process Automation, essa opção e o tipo de configuração já estão definidos. Todos os aplicativos usam o mesmo tipo de configuração. Os tipos de configuração variam de acordo com a release.
  - A opção "Referência de um diretório LDAP externo" do CA EEM Release 8.4 inclui o tipo de configuração do Microsoft Active Directory
  - A opção "Referência de um diretório LDAP externo" do CA EEM Release 12.5 inclui seu próprio conjunto de tipos de configuração, incluindo vários domínios do AD e uma floresta do AD.
- Se você estiver usando uma nova instância do CA EEM, considere usar este procedimento:
  1. Instalar o CA EEM e iniciar o CA EEM.
  2. Instalar o CA Process Automation. Durante a instalação, registre com o CA EEM que cria o aplicativo do CA Process Automation no CA EEM e ignore o teste de conectividade do CA EEM.
  3. Efetue logon no CA EEM com as credenciais do usuário EiamAdmin e o nome do aplicativo do CA Process Automation.
  4. Defina o armazenamento de usuários, e se você selecionar a opção Referência de um diretório LDAP externo, defina os detalhes.

     Para obter mais informações sobre como configurar usuários globais em um armazenamento de usuários referenciado no CA EEM, consulte a documentação do CA EEM. Consulte também os seguintes exemplos:
     - Referência a usuários globais e grupos globais do Microsoft Active Directory (na página 90) (CA EEM r8.4).
     - Referência a usuários globais de vários Active Directories (CA EEM r12.5) (na página 90)
  5. Enquanto estiver no CA EEM, configure os usuários do CA Process Automation. Consulte o tópico "Atribuir um grupo de aplicativos a um usuário global" no *Guia de Administrador de Conteúdo*.
  6. Opcionalmente, siga as instruções em Configurar o CA EEM para permitir que os usuários referenciados efetuem logon com seus nomes de email (na página 131).

Referência a usuários globais de um Microsoft Active Directory (CA EEM r8.4)

Durante a instalação do CA EEM r8.4, você pode selecionar a opção Referência de um diretório LDAP externo e, em seguida, selecionar Microsoft Active Directory como tipo.

Ao usar NTLM para segurança, marque a caixa de seleção Recuperar grupos do Exchange como grupos globais de usuários, conforme mostrado no exemplo a seguir:



Ao salvar as configurações, as seguintes mensagens de status são exibidas:

- A vinculação com o diretório externo foi bem-sucedida.
- Dados do diretório externo carregados.

Se NTLM estiver ativado e um usuário global efetuar logon pela primeira vez, uma caixa de diálogo Autenticação necessária será aberta. E o CA EEM usará o protocolo NTLM para autenticar os usuários.

Referência a usuários globais de vários Active Directories (CA EEM 12.5)

Durante a instalação do CA EEM r12.51, é possível configurar o CA EEM para fazer referência a vários Microsoft Active Directory ou a uma floresta do Active Directory.

Siga estas etapas:

1. Efetue logon no CA EEM como o usuário EiamAdmin. Especifique <Global> como o aplicativo.
2. Clique na guia Configurar e, em seguida, clique em User Store.
3. Selecione User Store na paleta User Store.
4. Para Usuários globais/Grupos globais, selecione Reference from an external LDAP Directory.

5. Selecione Multiple Microsoft Active Directory Domains na lista suspensa Tipo de configuração.
6. Clique em Add Directory e digite o primeiro nome do Active Directory no campo Nome.
7. Em Domain Settings, digite o nome do domínio no campo Domínio.
8. Digite o nome do host e o número da porta nos campos Host e Porta e, em seguida, clique na seta para a direita.

   A lista Selected Hostnames especifica onde o Active Directory está localizado.
9. Selecione o protocolo necessário na lista suspensa Protocolo.
10. Para DN Base (Distinguished Name - Nome Diferenciado), digite um valor sem espaços. O valor especifica o diretório LDAP externo que contém dados para os usuários globais e os grupos globais. No exemplo a seguir, o valor OU= limita os grupos globais que são carregados para aqueles na unidade organizacional especificada.

    `OU=myorganizationalunit,DC=foo,DC=com`
11. Especifique as credenciais que o CA EEM deve usar para acessar o domínio e a unidade organizacional que foram especificados. Esse usuário deve ser um integrante do domínio e da unidade organizacional que foram especificados para o DN Base.
    a. Para DN do usuário, digite o nome comum do usuário para conexão com o diretório LDAP externo. Use o caractere de escape (\) antes de uma vírgula entre partes do nome comum. Por exemplo,

       `CN=nome\,sobrenome,DC=foo,DC=com`
    b. Digite a senha associada ao nome comum especificado para o DN do usuário em Senha do usuário e Confirmar senha.
12. Preencha a configuração avançada ou aceite os padrões.
13. Repita as Etapas de 6 a 12 para cada AD para referência.
14. Clique em Salvar.

    Ao salvar as configurações, as seguintes mensagens de status são exibidas:
    - A vinculação com o diretório externo foi bem-sucedida.
    - Dados do diretório externo carregados.

Pré-requisitos do planejamento de portas

As portas são configuradas durante a instalação. Ao configurar portas de rede, aceite os padrões, exceto quando:

- A porta padrão estiver sendo usada por outro aplicativo no host.
- Uma restrição de firewall estiver impedindo a comunicação com a porta padrão.

Revise o uso das portas em Portas usadas pelo CA Process Automation (na página 223) e planeje substituições para quaisquer portas que estejam em uso em sua rede ou no host aplicável. Com exceção da porta para os agentes e para o CA EEM, todas as outras propriedades são armazenadas no arquivo OasisConfig.properties em *install_dir*/server/c2o/.config. Quando ocorre um conflito após a instalação, é possível modificar esse arquivo manualmente.

Instalação interativa do orquestrador de domínio

A instalação do orquestrador de domínio do CA Process Automation depende da presença de determinados componentes. Portanto, a instalação do CA Process Automation é realizada em duas principais etapas:

1. Instalando o software de terceiros.
2. Instalando o orquestrador de domínio.

As duas etapas devem sempre ser executadas na instalação, reinstalação ou atualização do CA Process Automation.

A instalação pode ser executada a partir da mídia física ou a partir de uma cópia feita a partir da mídia física ou obtida por download.

Você poderá sair do processo de instalação a qualquer momento. Se você cancelar, uma mensagem pop-up de confirmação será exibida. Caso você confirme o cancelamento, as etapas de instalação executadas até aquele instante serão revertidas.

Se você tiver um balanceador de carga, é recomendável configurar o orquestrador de domínio como um orquestrador agrupado, mesmo que você não tenha planos de agrupamento no momento. Se você decidir agrupar posteriormente e não tiver configurado o orquestrador de domínio como agrupado, deverá reinstalar o orquestrador de domínio para obter suporte a agrupamentos. Para detalhes, consulte os tópicos:

- Pré-requisitos do balanceador de carga NGINX (na página 36).
- Pré-requisitos do balanceador de carga F5 (na página 53).
- Pré-requisitos do balanceador de carga do Apache (na página 257).

Instalações subsequentes exigirão a configuração de determinados valores configurados durante a instalação do orquestrador de domínio. Por exemplo, algumas senhas devem ser inseridas novamente durante a atualização ou a instalação de outros orquestradores. Uma maneira simples de se manter um registro dos valores inseridos é criar um plano para senhas antes de iniciar a instalação interativa. Por exemplo, registre as senhas dos seguintes componentes e também quaisquer senhas específicas do servidor de banco de dados.

- Certificado do CA Process Automation.
- Certificado do CA EEM.
- Banco de dados de repositório.
- Banco de dados de relatórios.
- Banco de dados de tempo de execução.
- Administrador do CA EEM.

Mais informações:

Instalação autônoma do orquestrador de domínio (na página 118)

Instalar o software de terceiros

Comece a instalação do CA Process Automation instalando o software de terceiros. Quando essa instalação é concluída, a instalação do orquestrador é iniciada automaticamente.

Siga estas etapas:

1. Insira o DVD1 da mídia de instalação do CA Process Automation em uma unidade. Como alternativa, procure o local onde as pastas DVD1 e DVD2 que contêm os arquivos de instalação foram copiadas.
2. Execute o programa de instalação adequado para sua plataforma e mídia:
   - **Windows:** Domain_Installer_windows.bat
   - **Linux ou UNIX**: Domain_Installer_unix.sh

   Esses arquivos chamam o instalador de terceiros e, em seguida, o instalador do orquestrador de domínio.
3. Selecione o idioma preferencial na caixa de diálogo Seleção de idioma.

   Isso define o idioma padrão. Independentemente do idioma selecionado, o CA Process Automation é instalado com suporte a todos os locais disponíveis.

   Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation é exibido.
4. Clique em Avançar para iniciar a instalação dos componentes de terceiros.

5. Leia o contrato de licença. Para aceitá-lo, selecione Eu aceito os termos do Contrato de Licença e clique em Avançar.
6. Clique em Avançar para instalar os componentes no diretório de destino padrão. Ou, vá até um diretório diferente e, em seguida, clique em Avançar.

   O instalador criará a pasta automaticamente se ela não existir. Um mínimo de 8 GB de espaço em disco é necessário.

   Importante: certifique-se de que a estrutura de pastas do CA Process Automation, incluindo o local de instalação, não exceda 255 caracteres. A CA Technologies recomenda manter o caminho de instalação (*install_dir*) em 64 caracteres ou menos.

   A lista de pré-requisitos de terceiros é exibida. Os pré-requisitos de terceiros para o orquestrador de domínio incluem a Instalação do JBoss, a Instalação do Hibernate e a Instalação do JDBC Jar. No CA Process Automation r 4.2, o serviço de mensagens do ActiveMQ é usado com o JBoss 5.1.
7. Clique em Avançar e monitore a instalação do JBoss e dos componentes de terceiros.

   A Instalação do JDBC Jars é exibida.

8. Selecione um ou mais aplicativos de servidor de banco de dados para uso em acesso interno aos bancos de dados do CA Process Automation e especifique o caminho para o arquivo jar do driver do JDBC apropriado. Em seguida, clique em Avançar.

   - MySQL - Vá até um arquivo jar do driver do JDBC que você baixou anteriormente para MySQL. Por exemplo:

     `...`*`your_dir`*`\mysql-connector-java-5,1.19-bin.jar`

   - MS SQL - Aceite o caminho padrão para o arquivo jar do driver do JTDS JDBC no disco de instalação DVD1. Por exemplo:

     `...\DVD1\drivers\jtds-1.3.jar`

     (Opcionalmente, você pode ir até um arquivo jar do driver do JDBC diferente).

   - Oracle - Aceite o caminho padrão para o arquivo jar do driver do JDBC no disco de instalação DVD1. Por exemplo:

     `...DVD1\drivers\ojdbc14.jar`

     (Opcionalmente, você pode ir até um arquivo jar do driver do JDBC diferente).

   Observação: é necessário especificar pelo menos um driver do JDBC. Especificar vários drivers do JDBC para a comunicação interna geralmente não é necessário. Durante a instalação do orquestrador de domínio, é possível instalar drivers adicionais do JDBC para uso por outros orquestradores ou agentes com os operadores do banco de dados (anteriormente o módulo JDBC).

9. Quando Concluindo o Assistente de instalação do CA Process for exibido, insira o DVD2 de instalação do CA Process Automation ou substitua o DVD1 pelo DVD2 no campo. (Como alternativa, vá até o diretório que contém os arquivos da mídia de instalação DVD2.) Em seguida, clique em Concluir.

   O instalador de terceiros passa o controle para o instalador do orquestrador de domínio do CA Process Automation. Pode haver um curto intervalo em que a interface de usuário do instalador de terceiros será fechada e a interface de usuário de instalação do domínio do CA Process Automation ainda não terá aparecido. Isso é normal.

Instalar o orquestrador de domínio

Depois que o instalador de terceiros instalar os componentes de terceiros, o instalador copiará os arquivos de instalação do CA Process Automation para o host e iniciará o instalador do orquestrador de domínio.

Esta seção descreve como instalar um orquestrador de domínio não agrupado ou o primeiro nó de um orquestrador de domínio agrupado.

Siga estas etapas:

1. Na página Bem-vindo, clicar em Avançar.
2. Aceite o contrato de licença e clique em Avançar.
3. Verifique se o caminho exibido é o caminho para o diretório inicial do Java. Se o caminho para o diretório inicial do Java não for exibido, execute as seguintes etapas:
   a. Clique em Procurar
   b. Navegue até o local correto
   c. Selecione o JDK (Java Development Kit - Kit de Desenvolvimento Java) para uso. Por exemplo, selecione:

      ```
      C:\Arquivos de programas\Java\jdk1.7.0_21
      ```

   d. Clique em Avançar.

   O JDK é validado.
4. Monitore o progresso à medida que os arquivos são copiados.
5. Para configurar o CA Process Automation para uso com o CA SiteMinder, verifique se todos os pré-requisitos do CA SiteMinder foram atendidos. Em seguida, preencha os seguintes campos na tela Configuração de domínio do CA Process Automation:

   Configurar o SSO (Single Sign-On - Logon único)

   Marque essa caixa de seleção para configurar o CA SiteMinder com o orquestrador de domínio.

   Verifique se o WebAgent do CA SiteMinder está configurado com o mesmo balanceador de carga do Apache usado para o CA Process Automation.

   Tipo de autenticação SSO

   Selecione **Cabeçalho** como o tipo de autenticação quando o CA SiteMinder estiver configurado.

   O tipo de autenticação determina como o CA Process Automation é informado sobre a ID do usuário, quando um usuário for conectado por meio do CA SiteMinder. Os usuários podem selecionar os valores padrão preenchidos na lista Tipo de autenticação SSO.

Parâmetro de autenticação SSO

Especifica o nome do parâmetro de autenticação quando o CA SiteMinder estiver configurado.

Aceite os valores padrão ou insira novos valores, dependendo da configuração do CA SiteMinder.

- Selecione **sm_user** como o Parâmetro de autenticação SSO para IIS.
- Selecione **SM_User** como o Parâmetro de autenticação SSO para Apache.

Tipo de servidor

Especifica o tipo de instalação como novo orquestrador.

6. Selecione a ação apropriada:

   - Se você planeja configurar um orquestrador de domínio agrupado, leia as instruções e, em seguida, conclua esta tela de configuração.
   - Se estiver configurando o orquestrador de domínio para ser usado com o CA SiteMinder, leia as instruções e, em seguida, conclua esta tela de configuração.

   Configurar o balanceador de carga

   Especifica se é preciso instalar o orquestrador de domínio com o potencial para agrupamento.

   Selecionado

   Instale o orquestrador de domínio com o potencial para agrupamento. Antes de selecionar essa opção, verifique se você concluiu o tópico Pré-requisitos do balanceador de carga NGINX (na página 35) ou o Pré-requisitos do balanceador de carga F5 (na página 53).

   Desmarcado

   Instale o orquestrador de domínio sem o potencial para agrupamento.

   Nó de trabalho do balanceador de carga

   Define o nome do Nó de funcionário do balanceador de carga. Como a primeira instalação do orquestrador de domínio é o primeiro nó no agrupamento, esse valor, em geral, é node1.

   Se o Apache for o seu balanceador de carga, sua entrada deverá coincidir com o nome do nó na variável worker.*nodename*.host associada a esse host no arquivo do Apache *apache_install_dir*\conf\workers.properties. No exemplo a seguir, o valor da variável, **node1**, é o valor a ser atribuído aqui.

   `worker.`**`node1`**`.host=`*`DomainOrchestratorHostName`*

   Se o arquivo workers.properties tiver especificado worker.**abc**.host, você digitaria **abc**.

   Se F5 for o seu balanceador de carga, aceite o padrão. (O valor dos nós de funcionário não é relevante para o F5, portanto, não ocorre uma ligação com os pré-requisitos do F5 que você executou.)

   Padrão: node1 (Caracteres especiais, incluindo traços, não são suportados.)

Nome do host público

Especifica o nome do host público para o servidor Apache, o servidor NGINX ou o servidor F5. Por exemplo:

`loadbalancerhost.mycompany.com`

- Defina esse campo como o FQDN do IIS/Apache em que o WebAgent do CA SiteMinder está configurado, se você marcou a caixa de seleção Configurar Single Sign-On (SSO).
- Defina esse campo como o FQDN do balanceador de carga NGINX, F5 ou do Apache, se tiver marcado a caixa de seleção Configurar balanceador de carga sem a opção Configurar SSO (Single Sign-On).

Número da porta do host público

Define a porta HTTP para o IIS/Apache (o host público) ou o host do F5 se a caixa de seleção Suporte à comunicação segura estiver desmarcada.

Se você alterar esse valor durante a instalação e configuração do balanceador de carga NGINX, F5 ou do Apache, atualize esse valor de forma correspondente. Essa porta e o valor de Nome do host público são usados para navegar para o CA Process Automation. Por exemplo:

`http://public-host-name:80/itpam`

Padrão: 80

Porta segura do host público

Define a porta HTTPS para o host público especificado se a caixa de seleção Suporte à comunicação segura estiver marcada.

Essa porta é parte do URL usada para acessar os serviços web do CA Process Automation. Essa porta e o valor de Nome do host público são usados para navegar para o CA Process Automation. Por exemplo:

`https://public-host-name:443/itpam`

Padrão: 443

Suporte a comunicação segura

Especifica se o balanceador de carga (F5, NGINX ou Apache) usa HTTPS para comunicação segura.

Selecionado

Indica que o IIS ou Apache (o host público) usa HTTPS para se comunicar.

Observação: se você executou as etapas de "Configurar comunicação segura" para Apache, selecione esta opção.

Indica que o F5 usa HTTPS para se comunicar.

Desmarcado

Indica que o IIS ou Apache (o host público) usa HTTP para se comunicar.

Indica que o F5 usa HTTP para se comunicar.

7. Clique em Avançar.
8. No campo Empresa, digite o nome da sua empresa e, em seguida, clique em Avançar.

   O CA Process Automation exibe a entrada como o valor Este produto está licenciado para quando você clica em Ajuda, Sobre.
9. Digite uma senha do certificado, em seguida, digite-a novamente e então clique em Avançar.

   Senha do certificado

   Define a senha que controla o acesso às chaves usadas para criptografar senhas e outros dados críticos. Use a mesma senha ao instalar qualquer outro orquestrador ou ao adicionar nós de agrupamento para um orquestrador. A senha do certificado é específica para um único domínio do CA Process Automation.

   Confirmar senha do certificado

   Corresponde a sua entrada neste campo com a sua entrada no campo Senha do certificado para verificar a senha.

   Importante: Na página Definir senha do certificado, antes de clicar em Avançar, grave sua entrada Senha do certificado em um local seguro para referência futura. Essa mesma senha do certificado é necessária ao atualizar o orquestrador de domínio e outros orquestradores (incluindo nós de agrupamento) para uma nova release.

10. (Somente no Windows) Especifique as seguintes preferências do menu Iniciar e, em seguida, clique em Avançar.

    [Nome da pasta do menu Iniciar]

    Define o nome da pasta no menu Iniciar do CA Process Automation se você tiver desmarcado a caixa de seleção Não criar uma pasta no menu Iniciar. Aceite o padrão ou digite o nome da pasta no menu Iniciar para o CA Process Automation.

    Padrão: CA Process Automation 4.0

    Create shortcuts for all users

    Especifica se o nome da pasta do menu de atalho especificado é exibido para todos os usuários que efetuarem logon no servidor com o orquestrador de domínio do CA Process Automation.

    Selecionado: exibe os atalhos.

    Desmarcado: não exibe os atalhos.

    Não criar uma pasta no menu Iniciar

    Especifica se deve ser criada uma entrada para o CA Process Automation no menu Iniciar.

    Selecionado: cria uma entrada no menu Iniciar para o CA Process Automation.

    Desmarcado: não cria uma entrada no menu Iniciar para o CA Process Automation.

11. Preencha os seguintes campos para definir como o orquestrador de domínio se comunica com outros componentes e aplicativos do CA Process Automation e, em seguida, clique em Avançar.

    Host do servidor

    Define uma das seguintes propriedades:

    - O nome do host ou o endereço IP do sistema de host em que o orquestrador de domínio é implantado.
    - O Alias de DNS que resolve para o sistema do host.

    Nome de exibição

    Especifica o nome do orquestrador de domínio exibido no navegador de configuração do CA Process Automation.

    - Se você não configurar um balanceador de carga, o Nome de exibição será o mesmo que o Nome do host do servidor.
    - Se você configurar um balanceador de carga, o Nome de exibição será o FQDN do servidor no qual o balanceador de carga está instalado.

Suporte a comunicação segura

Especifica se a comunicação com o CA Process Automation é segura, em oposição à comunicação básica padrão. Este valor controla se a porta HTTP ou a porta HTTPS está ativada.

Selecionado: usa o protocolo HTTPS para comunicação.

Desmarcado: não usa o protocolo HTTPS para comunicação. Em vez disso, usa HTTP.

Porta do servidor

Define a porta que o orquestrador de domínio usa para se comunicar com outros orquestradores e agentes.

Padrão: 80 (básico: HTTP) ou 443 (protegido: HTTPS)

Porta do HTTP

Define a porta HTTP que é usada para o servidor da web se a caixa de seleção Suporte à comunicação segura estiver desmarcada.

Observação: esta porta é parte do URL usado para acessar os serviços web do CA Process Automation e a tela de logon do CA Process Automation.

Padrão: 8080

Porta do HTTPS

Quando você seleciona Suporte à comunicação segura, esse campo especifica a porta usada no URL que acessa os serviços web do CA Process Automation e a interface de usuário baseada no navegador do CA Process Automation.

Padrão: 8443

Observação: selecione "Suporte à comunicação segura" para permitir a entrada nesse campo.

Porta do JNDI

Define a porta do servidor de nomenclatura do Java que o servidor da web usa.

Observação: esta porta não deve ser acessada de fora desse sistema de host.

Padrão: 1099

Porta do RMI

Define a porta RMI que o servidor da web usa.

Observação: esta porta não deve ser acessada de fora desse sistema de host.

Padrão: 1098

Porta do SNMP

Define a porta de escuta de interceptação de SNMP para o CA Process Automation.

Padrão: 162

12. Aceite o caminho padrão ou vá até um diretório temporário para executar os scripts. Clique em Avançar.

    Esse diretório deve ser gravável por todos os usuários.

13. Preencha os seguintes campos para definir as configurações do PowerShell e, em seguida, clique em Avançar.

    Definir a diretiva de execução do PowerShell

    Especifica se é preciso ativar o uso do PowerShell.

    Selecionado: ativa o uso do PowerShell, definindo a diretiva de execução do PowerShell no caminho especificado como Remote Signed.

    Desmarcado: não permite o uso do PowerShell.

    Caminho do PowerShell na máquina host

    O CA Process Automation detecta automaticamente o caminho do PowerShell.

    Observação: quando você clica em Avançar, o programa de instalação valida o caminho do PowerShell fornecido.

14. Defina as configurações de segurança do CA EEM. A ordem em que os campos são apresentados nesta etapa tem como base as dependências, em vez da ordem dos campos exibida na interface do usuário.

    a. Preencha os seguintes campos obrigatórios:

    EEM Server

    Define o FQDN do servidor do CA EEM que o CA Process Automation usa para autenticar e autorizar os usuários do CA Process Automation. Se você estiver configurando o EEM para alta disponibilidade (HA), poderá definir também um servidor de backup do CA EEM. Use uma vírgula como o delimitador entre os nomes de servidor.

    Nome do aplicativo EEM

    Define como o nome do aplicativo do CA Process Automation é exibido no CA EEM. Se você usar o mesmo servidor do CA EEM com vários domínios do CA Process Automation, cada um deles deverá ter um nome de aplicativo do EEM exclusivo. O nome que você digitar aqui será exibido na lista suspensa da página de logon do servidor do CA EEM.

    Se você estiver atualizando o produto, este campo já estará preenchido com o valor usado na instalação inicial. Esse valor preserva as atribuições do grupo de usuários, as diretivas personalizadas e os grupos personalizados do CA EEM. O CA EEM usa esse valor para identificar esse domínio do CA Process Automation.

    Padrão: Process Automation

    Usar certificado compatível com FIPS

    Especifica se certificados compatíveis com FIPS serão usados ou não. Essa configuração deve corresponder à configuração do CA EEM para o modo FIPS.

    Observação: para determinar a configuração do CA EEM para FIPS, clique em Sobre no CA EEM; a opção Especificações do produto inclui FIPS desativado ou FIPS ativado.

    Marcado: o modo FIPS está definido como Ativado no CA EEM.

    Desmarcado: o modo FIPS está definido como Desativado no CA EEM.

b. Especifique que *deseja registrar* o nome do aplicativo especificado para este domínio do CA Process Automation com o CA EEM após concluir essa página. O processo de registro gera certificados compatíveis com FIPS ou não compatíveis com FIPS, com base na seleção feita. Essa caixa de seleção será exibida acima do botão Registrar. A configuração normal é a caixa de seleção marcada.

Registrar o aplicativo no CA EEM

Especifica se é necessário registrar o valor de Nome do aplicativo do EEM para o CA Process Automation com o CA EEM e gerar o certificado que o CA Process Automation usa para se conectar ao seu aplicativo no servidor do CA EEM. O CA EEM SDK lida com a conexão. Se solicitado, indique que deseja atualizar o aplicativo do CA Process Automation no CA EEM.

Selecionado: ativa o botão Registrar. (Consulte a Etapa 16.) Desativa o campo Arquivo do certificado do EEM. Para uma nova instalação de um orquestrador de domínio, sempre marque essa caixa de seleção. Quando preencher os campos de Configurações de segurança do EEM, clique em Registrar.

Desmarcado: desativa o botão Registrar. Ativa o campo Arquivo do certificado do EEM.

c. Para uma nova instalação, preencha o campo a seguir apenas se não estiver registrando o aplicativo no CA EEM. Clique em Procurar e encontre o local do arquivo do certificado. Depois que o arquivo do certificado for carregado, o instalador o colocará neste diretório:

`install_dir/server/c2o/.c2orepository/public/certification`

Observação: se você estiver atualizando o produto, esse campo será preenchido automaticamente com o caminho para o arquivo do certificado.

Arquivo do certificado do EEM

Define o arquivo do certificado do CA EEM a ser usada para o CA Process Automation. Geralmente, você pode aceitar o valor padrão.

Padrões:

PAM.cer se você marcou a caixa de seleção Usar o certificado compatível com FIPS.

PAM.p12 se você desmarcou a caixa de seleção Usar certificado compatível com FIPS.

d. Preencha um dos seguintes campos, se necessário.

Arquivo de chave do certificado

Se necessário (consulte as Observações), clique em Procurar e encontre o local da chave do certificado, por exemplo, o arquivo PAM.key. Depois que o arquivo do certificado for carregado, o instalador o colocará neste diretório:

install_dir/server/c2o/.c2orepository/public/certification

Observações:

- Se esta for uma nova instalação, esse campo não será obrigatório se você estiver usando o FIPS e pretender registrar. (O processo de registro gera o arquivo de chave do certificado com o certificado.)
- Se esta for uma nova instalação, esse campo será obrigatório se você estiver usando o FIPS e não pretender registrar.
- Se estiver fazendo a atualização, esse campo será preenchido com o caminho para o arquivo de chave.

Senha do certificado do EEM

Obrigatória se você não estiver usando o FIPS. Define a senha do certificado do CA EEM. Essa senha protege o certificado PAM.p12; o CA Process Automation precisará dessa senha para abrir e usar o certificado PAM.p12.

e. Preencha os campos a seguir apenas se você configurar o CA EEM para fazer referência a usuários a partir de um diretório LDAP externo. Caso contrário, ignore esta etapa.

Domínio padrão do Active Directory

(Aplicável apenas se você planejar referenciar vários domínios do Active Directory ao configurar o CA EEM Release 12.51. Consulte a Etapa 17.) Especifica o domínio do AD a ser usado como o domínio padrão. Os usuários do CA Process Automation que pertencem ao domínio especificado podem efetuar logon no CA Process Automation com seu nome de usuário não qualificado. Os usuários que pertencem a outros domínios do AD devem especificar o nome da entidade principal (*domínio**nome_de_usuário* ou *nome_de_usuário*@*domínio*) e a senha ao efetuar logon no CA Process Automation. Essa entrada deve coincidir com a entrada do campo Domínio para um dos vários domínios do AD que você configurar para o armazenamento de usuários referenciado pelo CA EEM.

O CA EEM deve ser adequadamente configurado para autenticar com o formato nome_de_usuário@domínio do nome da entidade principal.

Observação: consulte o tópico Configurar o CA EEM para permitir que os usuários referenciados efetuem logon com seus nomes de email (na página 131).

Ativa a Autenticação de passagem NTLM

Especifica se o CA EEM usa o protocolo NTLM para autenticar usuários do CA Process Automation.

Selecionado: ativa a autenticação de passagem de NTLM. O CA EEM usa o protocolo NTLM para autenticar usuários que navegam para o CA Process Automation.

Desmarcado: desativa a autenticação de passagem NTLM. Os usuários que navegam para o CA Process Automation devem digitar credenciais na caixa de diálogo de logon do CA Process Automation. O CA EEM valida as credenciais com os Microsoft Active Directories referenciados para usuários autenticados.

15. Registre o valor de Nome do aplicativo do EEM configurado com o CA EEM ou ignore o registro. O processo de registro gera certificados do CA Process Automation com o comprimento obrigatório.

    - Se esta for uma nova instalação, clique em Registrar, preencha os campos a seguir na janela Credenciais do EEM e clique em OK. Clique em OK quando a confirmação de aplicativo registrado for exibida.

      Nome de usuário do administrador do EEM

      Define o nome de usuário do administrador do CA EEM. Tipo **EiamAdmin**.

      Senha do Administrador do EEM

      Especifica a senha para a conta de usuário EiamAdmin. Se tiver instalado o CA EEM, digite a senha criada para o usuário EiamAdmin. Caso contrário, entre em contato com o administrador do CA EEM para obter a senha.

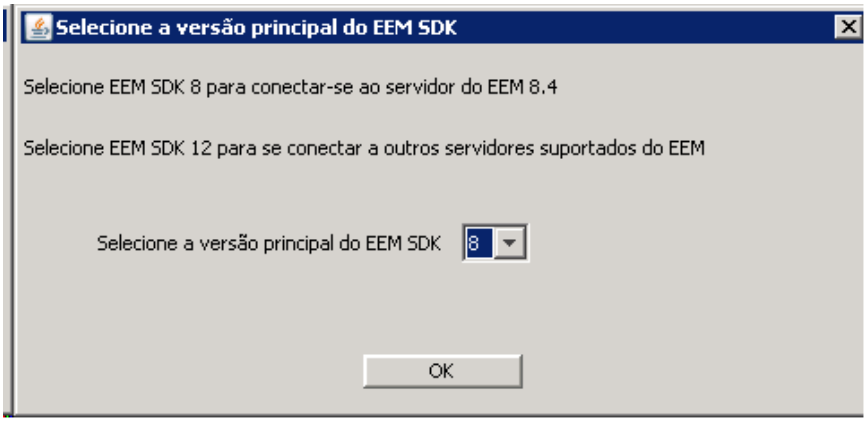
    - Se estiver usando certificados compatíveis com FIPS, os novos certificados PAM.cer e PAM.key substituirão os certificados existentes, se houver algum. Se não estiver usando certificados compatíveis com FIPS, o novo PAM.p12 substituirá o certificado existente no CA Process Automation, se houver algum. Esse certificado é protegido pela senha digitada no campo Senha do certificado do EEM. O campo Arquivo do certificado do EEM é preenchido com um caminho e com o nome do arquivo, de forma semelhante a este exemplo:

      `install_dir/server/c2o/.c2orepository/public/certification/PAM.p12`

      Observação: os certificados não serão gerados novamente se for solicitado que você decida se deseja atualizar o aplicativo do CA Process Automation no CA Embedded Entitlements Manager e você optar por *não* fazer a atualização.

A seguinte lista com marcadores descreve os casos de uso:

- Nova instalação com registro: o processo de instalação detecta a versão do servidor do CA EEM e escolhe o SDK apropriado.
- Nova instalação sem registro: o processo de instalação solicitará que você escolha um SDK com base na versão da release do CA EEM. Se você não souber qual é a versão da release do servidor do CA EEM, efetue logon no CA EEM e verifique as informações em Sobre.



16. (Opcional) Se desejar testar as configurações do CA EEM e tiver configurado o CA EEM para referenciar a partir de um diretório externo, é necessário criar primeiro um usuário de teste. Um usuário de teste é um usuário que você recupera de um Active Directory e, em seguida, atribui ao grupo PAMAdmins. Siga estas etapas:

    a. Navegue até o CA EEM que o CA Process Automation usa. Use o seguinte URL:

       `https://nome_do_host:5250/spin/eiam`

       A caixa de diálogo do CA Embedded Entitlements Manager é aberta.

    b. Na lista suspensa Aplicativo, selecione o nome que você configurou no campo Nome do aplicativo do EEM.

    c. Digite EiamAdmin e a senha do administrador do CA EEM que você configurou.

    d. Clique em Efetuar logon.

    e. Clique na guia Gerenciar identidades.

    f. Em Pesquisar usuários, onde a opção Usuários globais está selecionada, selecione Sobrenome ou Nome e digite seu nome ou sobrenome no campo Valor. Em seguida, clique em Ir. (Valores parciais são aceitos).

       O nome aparece em Usuários no painel Usuários.

    g. Clique duas vezes no nome para exibir a conta de usuário carregada.

       Sua conta de usuário possui duas seções de Detalhes do usuário. A seção superior permite definir um grupo para sua função no CA Process Automation. A seção inferior, Detalhes de usuário global, contém informações do diretório externo.

    h. Clique no botão Adicionar detalhes do usuário do aplicativo na seção superior.

       A lista Grupos de usuários disponíveis contém um grupo para cada função padrão.

    i. Selecione PAMAdmins e clique na seta para a direita para mover esse grupo para a lista de grupos de usuários selecionados.

    j. Clique em Salvar.

    k. Clique em Logoff.

17. (Opcional) Teste as configurações do CA EEM. Esta etapa requer que você digite as credenciais de um usuário definido no CA EEM. Se você estiver usando o CA EEM como um diretório local (o padrão), poderá inserir as credenciais de um dos usuários padrão. Se o CA EEM apontar para um diretório externo, insira suas próprias credenciais (se tiver concluído a etapa anterior).

    a. Clique em Testar configurações do CA EEM.

    b. Se estiver usando o CA EEM como um diretório local e esta for uma nova instalação, digite pamadmin em Nome de usuário, digite pamadmin em Senha e clique em OK.

    c. Se estiver usando uma conta de usuário de referência a partir de um diretório externo, digite suas credenciais de usuário como definidas no diretório externo. Esta é a conta do usuário de teste que você criou na etapa anterior.

    A tela Verificar configurações do EEM exibe os seguintes campos:

    Conectar

    Indica se é possível estabelecer uma conexão com o servidor do CA EEM especificado com os valores fornecidos na tela de configurações do CA EEM.

    Limites: OK, Não está correto

    Observação: se o valor for avaliado como Não está correto, os campos a seguir não serão exibidos.

    O usuário fornecido pertence ao grupo de usuários

    Indica se o usuário pode ser autenticado, isto é, se o logon é permitido.

    Limites: OK, Não está correto

    O usuário é um administrador

    Indica se o usuário possui autorização para executar tarefas de administrador. Os integrantes do grupo PAMAdmins possuem essa autorização.

    Limites: Sim, Não

    Atualização do EEM

    Indica se o esquema do aplicativo do CA Process Automation no servidor do EEM está atualizado. Se a mensagem Não é necessário atualizar for exibida, clique em OK.

    Observação: este campo só será exibido quando o valor for Não está correto. Quando o valor for Não está correto, atualize a instância.

18. Depois que você revisar os resultados, clique em OK e, em seguida, clique em Avançar.

19. Preencha os campos a seguir para definir as configurações do banco de dados Biblioteca (ou seja, o banco de dados Repositório).

Tipo do banco de dados

Especifica o tipo do sistema do banco de dados. Selecione um tipo suportado na lista suspensa.

Valores: MySQL, MS SQL, Oracle

Observação: se a instalação for para uso em produção, a melhor prática é selecionar MS SQL ou Oracle. O MySQL é uma escolha adequada para um orquestrador de domínio com carga mais leve.

Nome de usuário

Define um nome de usuário autorizado a criar e acessar o banco de dados no servidor do banco de dados. A conta deve ter permissões para criar o banco de dados no servidor ou na propriedade (DBO) de um banco de dados existente. Os seguintes valores são preenchidos automaticamente com base na seleção do banco de dados:

- MS SQL: **sa**
- MySQL: **root**

Senha

Define a senha associada ao Nome de usuário especificado.

Servidor do banco de dados

Define o nome do host ou o endereço IP do servidor de bancos de dados.

- Se você tiver configurado o Tipo de banco de dados como MS SQL e tiver uma única instância do SQL Server no servidor host ou se tiver selecionado outro tipo de banco de dados, especifique o nome do host ou o endereço IP do servidor de banco de dados. (Esse nome é a instância padrão.)
- Se você tiver configurado o Tipo de banco de dados como MS SQL e tiver várias instâncias do SQL Server no servidor host, especifique a instância nomeada do SQL Server. Use o formato host\instância, por exemplo, *dbserver.mycompany*.com*pamdb.*
- Se você tiver configurado o Tipo de banco de dados como Oracle, forneça um nome de SID.

Porta do banco de dados

Define a porta de conexão configurada no servidor de banco de dados.

- Para MS SQL, a porta padrão é 1433.
- Para MySQL, a porta padrão é 3306.
- Para Oracle, a porta padrão é 1521.

Banco de dados do repositório

Define o nome do banco de dados no qual armazenar objetos da Biblioteca e outros dados.

Cada orquestrador pode ter seu próprio banco de dados do repositório ou da biblioteca. Também é possível compartilhar o banco de dados da biblioteca entre os orquestradores. Cada banco de dados deve ter um nome exclusivo. Considere a possibilidade de estabelecer uma convenção de nomenclatura para os bancos de dados do CA Process Automation com essa instalação inicial.

Jar do Driver

Define o arquivo JAR do driver do JDBC para o tipo de banco de dados especificado. A pasta de drivers na pasta DVD1 da mídia de instalação fornece drivers padrão para o Microsoft SQL Server e os servidores de banco de dados Oracle.

Padrões:

SQL Server: jtds-1.3.jar

Oracle: ojdbc14.jar

MySQL: clique em Navegar e então navegue para o arquivo JAR baixado (por exemplo, mysql-connector-java-5,1.18-bin.jar).

Agrupamento de banco de dados

Define as regras de classificação de dados para MS SQL e Oracle. Diferenciação de maiúscula e minúscula, ênfases, tipos de caracteres de kana e largura de caracteres podem ser parte do conjunto de regras. Este campo é uma lista suspensa. É uma prática recomendada para aceitar o valor padrão. Este campo não é aplicável para o MySQL.

Padrão: SQL_Latin1_General_CP1_CI_AS

Usar a sequência de caracteres da conexão

Marque esta caixa de seleção para fornecer uma sequência de caracteres da conexão para conectar ao banco de dados Oracle.

Observação: esta caixa de seleção está ativada apenas para o banco de dados Oracle.

Sequência de caracteres da conexão

Digite uma sequência de caracteres da conexão jdbc em um dos seguintes formatos:

`jdbc:oracle:thin:`*`DatabaseServer`*`:`*`PortNumber`*`:`*`DatabaseName`*

`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=`*`hostname`*`)(PORT=`*`portnumber`*`))`
`(CONNECT_DATA=(SERVICE_NAME=`*`serviceid`*`)))`

20. Clique em Testar configurações do banco de dados para testar a conectividade do CA Process Automation com o servidor de banco de dados especificado usando a porta do banco de dados e o arquivo jar especificados.

    Se uma mensagem indicar que os bancos de dados estão ausentes, feche a mensagem e clique em Criar banco de dados. Exceto para Oracle, os bancos de dados que o orquestrador requer que sejam criados durante a instalação.

    Criar banco de dados

    Criar o banco de dados de repositório se você especificou MS SQL ou MySQL.

    Observação: ao usar um servidor de banco de dados Oracle, você já criou o banco de dados do repositório como parte das tarefas de pré-requisito do servidor de banco de dados.

    Uma mensagem indica que um banco de dados foi criado com o nome fornecido. Clique em OK. Clique em Testar configurações do banco de dados novamente.

21. Clique em Avançar.

22. Digite as informações do banco de dados de tempo de execução, manualmente ou copiando as especificações das entradas do banco de dados do repositório. Clique em Criar banco de dados se o Tipo de banco de dados for MSSQL ou MySQL. Clique em Testar configurações do banco de dados.

    Os campos do banco de dados de tempo de execução são semelhantes aos campos de configuração de banco de dados para o banco de dados do repositório (biblioteca), exceto por dois campos. Consulte a Etapa 20 para obter descrições de outros campos.

    copiar do repositório principal

    Especifica se as configurações do banco de dados da biblioteca devem ser copiadas para a tela de configurações do banco de dados de tempo de execução.

    Selecionado: copia as configurações do banco de dados da biblioteca para essa caixa de diálogo. Esta opção pode poupar tempo, caso você esteja usando o mesmo servidor de banco de dados para ambos os bancos de dados do CA Process Automation. Se você selecionar essa opção, digite o nome do banco de dados de tempo de execução no campo Banco de dados de tempo de execução. Em seguida, clique em Testar configurações do banco de dados. Em seguida, clique em Criar banco de dados.

    Desmarcado: não copie as configurações do banco de dados da biblioteca para essa caixa de diálogo. Essa opção será apropriada se você estiver usando um tipo diferente de banco de dados para os dados de tempo de execução do que está usando para os registros da biblioteca.

    Banco de dados de tempo de execução

    Define o nome do banco de dados ou do esquema no qual as instâncias de tempo de execução estão armazenadas. Dois orquestradores não podem apontar para o mesmo banco de dados de tempo de execução. Digite um nome exclusivo.

    Padrão: pam

    Importante: Não é possível compartilhar um banco de dados de tempo de execução em orquestradores. Se você desinstalar e reinstalar o CA Process Automation, o banco de dados de tempo de execução que você configurar aqui não é alterado.

23. Clique em Avançar.

24. Configure o banco de dados de relatórios de uma das seguintes maneiras:

    - Se estiver usando o mesmo servidor de banco de dados para o banco de dados de relatórios que você está usando para o banco de dados de repositórios:

        a. Digite um nome exclusivo para o banco de dados de relatórios no campo Banco de dados de relatórios.

        b. Marque a caixa de seleção Copiar do repositório principal para inserir dados compartilhados automaticamente.

        c. Clique em Testar configurações do banco de dados.

        d. Se o Tipo de banco de dados for MS SQL ou MySQL, clique em Criar banco de dados.

    - Se estiver usando um servidor de banco de dados diferente para o banco de dados de relatórios que você está usando para o banco de dados de repositório:

        a. Digite um nome exclusivo para o banco de dados de relatórios no campo Banco de dados de relatórios.

        b. Desmarque a caixa de seleção Copiar do repositório principal.

        c. Selecione o tipo de banco de dados na lista suspensa Tipo de banco de dados.

        d. No campo Nome de usuário, digite um nome de usuário autorizado para criar e acessar o banco de dados no servidor de banco de dados. (Por exemplo, digite sa para MS SQL; digite root para MySQL).

        e. Clique em Testar configurações do banco de dados.

        f. Se o Tipo de banco de dados for MS SQL ou MySQL, clique em Criar banco de dados. (Não clique nesse botão se o banco de dados de relatórios for executado em um servidor de banco de dados Oracle).

    Consulte as seguintes descrições de campo:

    copiar do repositório principal

    Especifica se as configurações do banco de dados da biblioteca devem ser copiadas para a tela do banco de dados de relatórios. Os campos do banco de dados de relatórios são semelhantes aos campos de configuração de banco de dados para o banco de dados do repositório (biblioteca), exceto por dois campos. Consulte a Etapa 20 para obter descrições de outros campos.

    Selecionado: copia as configurações do banco de dados de repositório para essa caixa de diálogo. Essa opção pode economizar tempo, caso você esteja usando o mesmo servidor de banco de dados para ambos os bancos de dados do CA Process Automation.

    Desmarcado: não copie as configurações do banco de dados de repositório para essa caixa de diálogo. Essa opção será apropriada se você estiver usando um tipo diferente de banco de dados para os dados de relatório do que está usando para os registros de tempo de execução.

Banco de dados de relatórios

Define o nome do banco de dados de relatórios que armazena todos os relatórios gerados. Digite um nome exclusivo.

25. Clique em Avançar.
26. Selecione os arquivos JAR adicionais, geralmente, os drivers do JDBC que você deseja incluir na instalação.

    Por padrão, os drivers JDBC carregados na instalação de software de terceiros são exibidos e desmarcados. Você pode usar o botão Adicionar arquivos para adicionar mais arquivos JAR.

    Selecione cada arquivo JAR que você deseja implantar. Verifique se você selecionou todos os drivers que deseja implantar para uso do Operador JDBC em agentes e orquestradores do CA Process Automation. Use o botão Adicionar arquivos para adicionar mais drivers.

    Não é necessário para prever as necessidades de desenvolvedores para drivers do JDBC. Um administrador de domínio pode implantar os drivers do JDBC à medida que forem necessários.

    Observação: para obter mais informações sobre como adicionar e gerenciar recursos do agente e do orquestrador, incluindo arquivos JAR do JDBC, consulte o Guia do administrador de conteúdo.

    Quando estiver satisfeito com a seleção de arquivos JAR, clique em Avançar.
27. Monitore o andamento da instalação. O programa de instalação copia e assina todos os componentes do CA Process Automation. A instalação pode levar alguns minutos.
28. Clique em Concluir para sair do programa de instalação.

    A instalação do orquestrador de domínio está concluída.

    Observe que na primeira vez em que você iniciar o CA Process Automation após uma atualização ou instalação, poderá levar mais tempo devido ao ajuste do esquema de banco de dados realizado pelo produto. Um guia geral é 1 hora por GB de dados; no entanto, isso pode variar dependendo do fornecedor do DBMS, das especificações do computador e do volume de dados. Inicie o orquestrador (na página 138). Verifique a operação correta desse orquestrador inicial antes de prosseguir com a instalação ou atualização de outros componentes do sistema.

Instalação autônoma do orquestrador de domínio

O CA Process Automation oferece a opção de instalar o orquestrador de domínio de maneira silenciosa ou autônoma por meio do uso de um arquivo de resposta. O arquivo de resposta contém diversos parâmetros predefinidos para serem usados durante o processo de instalação. Depois de criar um arquivo de resposta, você pode editar e executar o arquivo de script de instalação para iniciar a instalação.

Um exemplo de arquivo de resposta foi fornecido na pasta raiz do DVD1. Recomenda-se que uma cópia desse arquivo seja usada como base para o seu arquivo de resposta.

Criar um arquivo de resposta

A primeira etapa na execução de uma instalação silenciosa do CA Process Automation é criar um arquivo de resposta.

Considere as seguintes observações sobre o arquivo de resposta:

- Não altere os nomes de variáveis, pois a instalação usa os nomes de variáveis existentes.
- Use barras (/) como separadores de diretório para especificar locais de pastas.
- Use o sinal de número (#) para comentar qualquer variável que você não desejar usar.
- Consulte o seguinte log de instalação para revisar erros:

  ```
  ${install_dir}/server/c2o/installation.log
  ```

Siga estas etapas:

1. Insira o Disc1 da mídia de instalação do CA Process Automation ou navegue até o local em que os arquivos de instalação foram copiados anteriormente a partir da mídia de instalação.
2. Abra a pasta do DVD1.

3. Abra o arquivo a seguir.

   `response.varfile`

4. Forneça os valores de parâmetro apropriados.

   O varfile inclui descrições do parâmetro. Por exemplo, para permitir que o CA EEM use o protocolo NTLM para autenticar usuários do CA Process Automation, use a seguinte configuração:

   `enableNTLM = true`

   Os parâmetros necessários podem ser encontrados aqui.

5. Salve o varfile no caminho que contém o arquivo de script de instalação silenciosa.

   O arquivo de resposta é criado.

Parâmetros necessários no response.varfile

Conforme mencionado anteriormente, um exemplo de arquivo de resposta foi fornecido na pasta raiz do DVD1. Os parâmetros necessários para a execução de uma instalação autônoma do CA Process Automation incluem a lista a seguir. Os parâmetros que não estão incluídos nessa lista são opcionais.

License

thirdPartyLicenseAccepted

licenseAccepted

Local de instalação

sys.installationDir

Local do Java

javaHome

Local do DVD2

domainInstallerDir

Modo de comunicação

isSecure (verdadeiro/falso)

Detalhes do banco de dados

- databaseType
- dbUserName
- databaseServer
- databasePortNumber
- libDb
- driver
- runtimeDbType
- runtimeDbUserName
- runtimeDbServer
- runtimeDbPort
- runtimeDb
- runtimeDriver
- reportingDbType
- reportingDbUserName
- reportingDbServer
- reportingDbPort

- reportingDb
- reportingDriver

Detalhes do CA EEM

- registerApplication (definido como verdadeiro para uma atualização)
- upgradeApplication (definido como verdadeiro para uma atualização)
- eiamServer
- eiamAppName
- eiamAdminUsrName
- eiamSDKLevel

Novos parâmetros do CA Process Automation Release 4.2:

nodeCommsV2Port

A porta usada para comunicações simplificadas do orquestrador de domínio.

eiamSDKLevel

A entrada para o nível de SDK do CA EEM.

#hasOracleConnectionString

Especifica se é necessário fornecer um URL de conexão. Isso é aplicável somente com o Oracle.

#dbOracleConnectionString

URL de conexão JDBC.

Exemplo:
`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<nome do host do banco de dados>) (PORT=<número da porta>))(CONNECT_DATA=(SERVICE_NAME=<libDb>))).`

Observação: as duas últimas entradas aparecerão três vezes; duas vezes para cada banco de dados. Esses parâmetros são aplicáveis somente se você selecionar o Oracle como seu banco de dados e usar uma sequência de caracteres de conexão.

Executar ou editar o arquivo de script de instalação silenciosa

Depois de criar o arquivo de resposta, use uma das seguintes opções para iniciar a instalação silenciosa:

- Execute o arquivo de script de instalação silenciosa e passe seus parâmetros por meio do prompt de comando. Essa opção é a melhor prática quando você está instalando um único orquestrador.
- Edite os parâmetros do arquivo de script de instalação, e em seguida, execute o script. Essa opção é a melhor prática quando você está instalando vários orquestradores.

Use o arquivo de script de instalação apropriado para o seu ambiente operacional:

Observação: para o UNIX, se você chamar o arquivo de script da instalação usando um cifrão ($) em um parâmetro, coloque uma barra invertida (\) antes do cifrão ($). Por exemplo, se a senha do banco de dados for 'abc$123', coloque a barra invertida (\) como 'abc\$123'.

Windows

Sintaxe

```
Silent_Install_windows.bat [Parameter1] [Parameter2]
[Parameter3]...
```

Uso:

```
Silent_Install_windows.bat -VcertPassword=a
-VeiamCertPass=eiamadmin -VeiamPassword=eiamadmin
-VdbPassword=sa -VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

UNIX

Sintaxe

```
Silent_Install_unix.sh [Parameter1] [Parameter2] [Parameter3]...
```

Uso:

```
Silent_Install_unix.sh -VcertPassword=a -VeiamCertPass=eiamadmin
-VeiamPassword=eiamadmin -VdbPassword=sa
-VreportingDbPassword=sa -VruntimeDbPassword=sa
-VeiamAdminPass=eiamadmin
```

Os scripts de instalação incluem os seguintes parâmetros:

-VcertPassword=*value*

Define a senha que controla o acesso às chaves que criptografam senhas.

-VeiamCertPass

Define a senha do certificado do CA EEM (por exemplo, pamadmin).

-VeiamPassword

Define a senha do banco de dados usada para objetos de automação (por exemplo, paradmin).

Observação: VeiamPassword é a senha de domínio do Windows.

-VdbPassword

Define a senha do banco de dados usada para automação (por exemplo, objectsroot).

-VreportingDbPassword

Define a senha do banco de dados de relatórios (por exemplo, root).

-VruntimeDbPassword

Define a senha do banco de dados usada em tempo de execução (por exemplo, root).

-VeiamAdminPass

Define a senha do administrador do CA EEM, em que o valor de nome do usuário é EiamAdmin (por exemplo, eiamadmin).

Importante: Os parâmetros de senha, independentemente de serem transmitidos pela linha de comando ou armazenados no arquivo de script de instalação, *não* são criptografados.

Após a conclusão da instalação, você poderá iniciar o orquestrador. Analise o installation.log quanto a quaisquer erros após a execução do script (install_dir\server\c2o).

Considerações sobre atualização (instalação silenciosa)

Antes de executar uma atualização autônoma para o CA Process Automation Release 4.2, localize o response.varfile na sua instalação atual do CA Process Automation.

Este arquivo pode ser encontrado aqui:

```
<install_dir>\server\c2o\.install4j\response.varfile
```

Você precisa dos valores dos parâmetros necessários (na página 120) para concluir a atualização para o CA Process Automation Release 4.2. Depois de obter esses valores, inicie a atualização autônoma com o mesmo comando como em uma nova instalação (na página 121).

Observação: os drivers jTDS são obrigatórios no CA Process Automation Release 4.2. jtds-1.3.1.jar está incluído na pasta de drivers do DVD1. Qualquer parâmetro do response.varfile de uma instalação anterior que inclua uma referência a um arquivo JAR do SQL deve ser substituído por um valor de jTDS no response.varfile do CA Process Automation Release 4.2.

Por exemplo, um response.varfile do CA Process Automation Release 3.1 pode incluir o seguinte parâmetro:

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drive
rs/sqljdbc.jar
```

No CA Process Automation Release 4.2, esse parâmetro se torna:

```
runtimeDriver=C:/Users/Administrator/Desktop/2013_11_11/DVD1/drive
rs/jtds-1.3.1.jar
```

Tarefas pós-instalação para o orquestrador de domínio

Execute as tarefas pós-instalação que forem aplicáveis.

- Se você reinstalou (não atualizou) o orquestrador de domínio para que pudesse definir a comunicação segura usando HTTPS, consulte Ativar a comunicação segura de dados para CA Process Automation existente (na página 170).
- Se tiver instalado o CA Process Automation pela primeira vez:
  - Verifique se os Pré-requisitos do planejamento de porta (na página 92) para configurar portas.
  - Configure os firewalls para comunicação bidirecional (na página 128).
- Para usar os operadores Bancos de dados para se conectar aos bancos de dados usando um RDBMS diferente do usado pelo CA Process Automation, instale os drivers para os operadores Bancos de dados (na página 129).

  Para usar a autenticação do Windows (segurança integrada) com JDBC para o MSSQL Server, instale os drivers para os operadores Bancos de dados (na página 129).
- Se tiver instalado o orquestrador de domínio em um servidor com o sistema operacional HP-UX, execute as etapas de configuração adicionais no HP-UX.
- Se você instalou o CA EEM com o Microsoft Active Directory como o diretório externo, o CA EEM pode autenticar usuários com o protocolo NTLM. Se você não optar por ativar a autenticação de passagem NTLM durante a instalação, poderá ativá-la manualmente agora. Consulte Ativar a autenticação de passagem NTLM após a instalação (na página 130).
- Tarefas como implantar os drivers para os operadores Banco de dados exigem que você reinicie o orquestrador de domínio.
  - Consulte o tópico Interromper o orquestrador (na página 137).
  - Consulte o tópico Iniciar o orquestrador (na página 138).
- Antes de configurar o primeiro administrador no CA EEM, é possível ir até o CA Process Automation e efetuar logon como administrador padrão.

  Consulte o tópico Ir até o CA Process Automation e efetuar logon como administrador padrão (na página 125).

Ir até o CA Process Automation e efetuar logon como administrador padrão

Muitos dos tópicos neste guia pressupõem que você tenha acesso à interface de usuário do CA Process Automation. Tarefas como implantar drivers, instalar orquestradores e adicionar nós são iniciadas na guia Configuração no CA Process Automation. Os administradores geralmente efetuam logon no CA Process Automation com suas próprias credenciais para executar essas tarefas.

Observação: para obter mais informações sobre a criação da sua própria conta de usuário, consulte o *Guia do Administrador de Conteúdo*.

Para estar disponível, o CA Process Automation requer as seguintes condições:

- O CA EEM em execução.
- O balanceador de carga, se usado, em execução.
- O serviço do orquestrador de domínio é iniciado. Para obter mais informações, consulte Iniciar o orquestrador (na página 138).

Para executar tarefas que requerem acesso ao CA Process Automation antes de você ter uma conta de usuário do CA Process Automation, efetue logon no CA Process Automation com as credenciais de administrador padrão.

Importante: As credenciais padrão de administrador não estão disponíveis se o CA EEM estiver configurado para usar o Microsoft Active Directory como um armazenamento de usuários. As credenciais padrão para cada função de usuário estão disponíveis somente se você tiver configurado o CA EEM para usar o armazenamento de usuários local para criar e armazenar contas de usuário.

Siga estas etapas:

1. Acesse o URL apropriado do CA Process Automation. Nos exemplos a seguir, *server* se refere ao servidor no qual um orquestrador de domínio não agrupado está instalado. Para um orquestrador de domínio agrupado, *server* se refere ao servidor com o balanceador de carga.

   - Para uma comunicação segura, use a sintaxe a seguir:

     `https://server:port/itpam`

     Exemplos:

     `https://domainOrchestrator_host:8443/itpam`

     `https://loadBalancer_host:443/itpam`

   - Para uma comunicação básica, use a sintaxe a seguir:

     `http://server:port/itpam`

     Exemplos:

     `http://domainOrchestrator_host:8080/itpam`

     `http://loadBalancer_host:80/itpam`

   A página de logon do CA Process Automation é exibida.

   Observação: se a autenticação NTLM estiver ativada e as suas credenciais de domínio corresponderem às credenciais da conta de usuário do CA EEM, a guia Início será exibida. Para oferecer suporte à autenticação NTLM no Mozilla Firefox, defina as configurações do navegador. Para obter mais informações, consulte o suporte do Mozilla.

2. Digite **pamadmin** para o nome de usuário.
3. Digite **pamadmin** para a senha.
4. Clique em Efetuar logon.

   O CA Process Automation é exibido. A guia Início é exibida.

5. Na lista suspensa Ajuda, clique em Biblioteca. Verifique se a biblioteca pode ser aberta a partir do Atendimento ao cliente da CA Technologies.
6. Se a biblioteca não abrir porque o acesso à internet não é fornecido no ambiente em que os usuários do CA Process Automation trabalham:

   a. Vá para um local da empresa com acesso à internet

   b. Vá até o URL da Biblioteca do CA Process Automation Release 04.20.00 https://support.ca.com/cadocs/0/CA%20Process%20Automation%2004%202%2000-ENU/Bookshelf.html.

   c. Clique no link Fazer download desta biblioteca.

   d. Mova a biblioteca do local de download para:

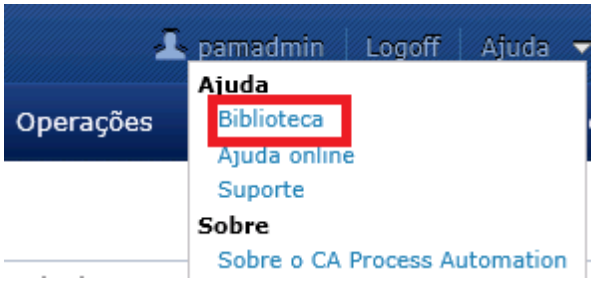
Tornar a biblioteca disponível para os usuários sem acesso à internet

Os usuários com acesso à internet podem abrir a documentação da biblioteca do CA Process Automation a partir do link Biblioteca no CA Process Automation. Este link acessa a biblioteca do CA Process Automation Release 4.2 publicada no Atendimento ao cliente da CA Technologies.

Os usuários sem acesso à internet precisam de ajuda para tornar a biblioteca do CA Process Automation disponível para eles. Ative o link Biblioteca fazendo download da biblioteca e movendo-a para um local que pegará a cópia do servidor local.

Siga estas etapas:

1. Ir até o CA Process Automation e efetuar logon como administrador padrão (na página 125).
2. Na lista suspensa Ajuda, clique em Biblioteca. Determine se a biblioteca pode ser aberta a partir do Atendimento ao cliente da CA Technologies.



3. Se a biblioteca não abrir porque o acesso à internet não é fornecido no ambiente em que os usuários do CA Process Automation trabalham:
   a. Vá para um local da empresa com acesso à internet
   b. Vá até o URL da Biblioteca do CA Process Automation Release 04.20.00 https://support.ca.com/cadocs/0/CA%20Process%20Automation%2004%202%2000-ENU/Bookshelf.html.
   c. Clique no link Fazer download desta biblioteca.
   d. Mova a biblioteca do local de download para:

      install_dir\server\c2o\.c2orepository\biblioteca

4. Na lista suspensa Ajuda, clique em Biblioteca. Verifique se a biblioteca é aberta.

Configure os firewalls para comunicação bidirecional

Os componentes do CA Process Automation podem ser acessados por meio de clientes da web. Consulte o tópico Portas usadas pelo CA Process Automation (na página 223) para obter detalhes sobre as portas usadas por cada componente em um sistema do CA Process Automation.

Você deve configurar os firewalls para permitir uma comunicação bidirecional. Uma comunicação bidirecional é necessária entre os seguintes pares de componentes:

- O orquestrador de domínio e o servidor de banco de dados usado para o banco de dados da biblioteca.
- O orquestrador de domínio e o servidor de banco de dados que ele usa para o banco de dados de relatórios.
- O orquestrador de domínio e o servidor de banco de dados que ele usa para o banco de dados de tempo de execução.
- O orquestrador de domínio e o CA EEM.
- Cada orquestrador e o servidor de banco de dados usado para o banco de dados da biblioteca.
- Cada orquestrador e o servidor de banco de dados que ele usa para o banco de dados de relatórios.
- Cada orquestrador e o servidor de banco de dados que ele usa para o banco de dados de tempo de execução.

Se você usar firewalls locais em máquinas host do orquestrador ou agente, certifique-se de que os executáveis do CA Process Automation podem ouvir e conectar bidirecionalmente através do firewall em cada host. Alguns programas de firewall baseado no host (como o Windows Firewall) permitem exceções para executáveis.

Instalar drivers para os operadores de bancos de dados

Os criadores do CA Process Automation podem usar operadores da categoria Banco de dados (anteriormente o módulo JDBC) para se conectar a vários RDBMSs (Relational Database Management System - Sistema de Gerenciamento de Banco de Dados Relacional). Quando a conexão é com um banco de dados MySQL, um banco de dados Oracle ou um banco de dados Microsoft SQL Server, os drivers corretos estão disponíveis. (A disponibilidade de todos os três drivers depende da seleção feita durante a instalação do orquestrador de domínio.) Quando a conexão é com um banco de dados a partir de outro fornecedor, você pode implantar o driver do JDBC para os operadores Banco de dados desse banco de dados na guia Configuração do CA Process Automation. Por exemplo, se um criador deseja usar os operadores Banco de dados para Sybase, um administrador implanta os drivers do JDBC para Sybase. Um administrador pode implantar os drivers do JDBC nos orquestradores ou em hosts com os agentes do CA Process Automation.

Observação: consulte o tópico "Como implantar drivers do JDBC para operadores do banco de dados" no capítulo Gerenciar recursos do usuário do *Guia de Administrador de Conteúdo* para obter os procedimentos.

Ativar a autenticação de passagem NTLM após a instalação

A autenticação de passagem NTLM permite que o CA EEM autentique usuários com o protocolo NTLM. Essa é uma alternativa para o uso de credenciais que os usuários digitam na caixa de diálogo de logon com base em formulário. Com a autenticação de passagem NTLM, a caixa de diálogo de logon é ignorada.

O procedimento a seguir *não* será aplicável se você já tiver ativado autenticação de passagem NTLM, por exemplo:

- Você selecionou a opção Ativar a autenticação de passagem NTLM durante instalação interativa do CA Process Automation.
- Você especificou enableNTLM=true em response.varfile usado para a instalar o CA Process Automation de maneira silenciosa.

É possível ativar a autenticação de passagem NTLM adicionando manualmente ntlm.enabled=true ao arquivo OasisConfig.properties. Use o procedimento a seguir apenas quando desejar ativar esse recurso, e não tiver feito isso na instalação.

Siga estas etapas:

1. Efetue logon como administrador no servidor em que o orquestrador de domínio está instalado.
2. Vá até a seguinte pasta, em que install_dir faz referência ao caminho em que o orquestrador de domínio está instalado:

   `install_dir/server/c2o/.config`
3. Abra o arquivo OasisConfig.properties com um editor.
4. Use Localizar para encontrar a seguinte propriedade: ntlm.enabled=
5. Altere o valor da propriedade para true, ou seja:

   `ntlm.enabled=true`
6. Salve o arquivo e saia.
7. Reinicie o serviço do orquestrador.
   a. Interrompa o orquestrador (na página 137).
   b. Inicie o orquestrador (na página 138).
8. Repita esse processo para cada orquestrador.

Interagir com a configuração de área de trabalho

Os orquestradores e agentes normalmente são executados como serviços de console e não precisam interagir com a área de trabalho. Se um orquestrador ou agente tiver de interagir com a área de trabalho do Windows, o serviço do orquestrador ou do agente deverá ser iniciado usando uma conta de usuário ou a conta do sistema local com a opção Permitir que o serviço interaja com a área de trabalho selecionada. Esta opção é selecionada por padrão quando um orquestrador ou agente é instalado. Como alternativa, esse serviço pode ser configurado usando o console de serviços nas Ferramentas administrativas do Windows. A caixa de seleção para permitir esse privilégio está sob a tag Efetuar logon na janela propriedades para o serviço.

Configurar o CA EEM para permitir que os usuários referenciados efetuem logon com seus nomes de email

Quando você instala o CA Process Automation, é possível configurar Usuários globais/Grupos globais na EEM Server Configuration como Referência de um diretório LDAP externo. É possível, em seguida, selecionar Multiple Microsoft Active Directory Domains e especificar os Microsoft Active Directories (ADs) nos quais os possíveis usuários do CA Process Automation são definidos. Durante uma instalação do CA Process Automation, você pode identificar o domínio do AD padrão. Os usuários que pertencem ao domínio do AD padrão podem efetuar logon no CA Process Automation com seus respectivos nomes de usuário e senhas. Os usuários que pertencerem a outros domínios do AD devem digitar seus respectivos nomes da entidade principal e senhas no logon. O formato padrão para um nome da entidade principal é *domínio**nome_de_usuário*.

Você pode configurar o CA EEM para autenticar os usuários do Active Directory com seus respectivos endereços de email, isto é, *nome_de_usuário@domínio*. Você configura o CA EEM para procurar o usuário usando userPrincipalName.

Siga estas etapas:

1. Efetue logon no CA EEM como o administrador do CA EEM e selecione o nome do aplicativo que você configurou durante a instalação do CA Process Automation.
2. Selecione a guia Configurar.
3. Na paleta User Store, selecione LDAP Attribute Mapping.

4. Crie um mapa de atributos com o mapa de atributos existentes, alterando o filtro de autenticação de usuário. Isto é, altere samaccountName para userPrinciaplName.
   a. Selecione Microsoft Active Directory na lista suspensa Mapping Name.
   b. No painel User Lookup, o User Search Filter é semelhante ao seguinte exemplo:

      ```
      (&(objectClass=user)(!(objectClass=computer)))
      ```

   c. Edite o campo User Authentication Filter, de forma que userPrincipalName substitua samaccountName. Veja os resultados do exemplo a seguir:

      ```
      (&(ObjectClass=user)(!(objectClass=computer)(userPrincipalName= ...
      ```

   d. {UserName} é definido da seguinte maneira:

      ```
      ))
      ```

5. Salve o mapa de atributos. Por exemplo, digite o nome **madAuthMail** no campo Mapping Name e, em seguida, clique em Salvar.
6. Os dados de User Attribute Mapping se parecem com os seguintes dados:

   Nome de usuário: sAMAccountName

   Nome: givenName

   Sobrenome: sn

   Nome de exibição: displayName
7. Na seção Geral da LDAP Directory Configuration, digite o nome do mapa de atributos que você criou na Etapa 5. Verifique se suas entradas se parecem com o seguinte texto:

   Nome: *domain*

   Attribute Map: madAuthMail

   Domínio: *domain*

   Selected Hostnames: *hostname:*389

   Protocolo: LDAP

   DN Base: ou=*mylocation*,dc=*mycompany*,dc=com

   DN do usuário: cn=*userid*,ou=Users,ou=*mylocation*,dc=*mycompany*,dc=com

   Senha do usuário: *passwordForUserid*

Pré-requisitos da sincronização de hora

É recomendável que você sincronize a hora do orquestrador de domínio com um servidor de tempo externo padrão. Isso prepara o orquestrador de domínio para o momento em que um nó de agrupamento é adicionado. Todos os nós de agrupamento para qualquer orquestrador devem ter a mesma hora do relógio, idealmente sincronizada com um servidor de tempo externo padrão. O balanceador de carga não realiza a sincronização de hora.

Mais informações:

Sincronizar a hora para um nó de agrupamento (na página 191)

Como instalar patches e conectores com o CA Process Automation 4.2

Esta seção descreve como instalar os conectores do CA Process Automation com o JBoss 5.1 em um host.

Os administradores podem instalar os conectores do CA Process Automation para permitir que o CA Process Automation interaja com outros produtos (produtos da CA e de terceiros) para automatizar os casos de uso corporativo. Cada conector atua como um módulo que contém um conjunto de operadores. Os operadores interagem com APIs de outros produtos e são usados para criar os fluxos do CA Process Automation.

Como pré-requisito, verifique se você instalou o CA Process Automation no host. O executável do conector do CA Process Automation está presente no host.

Importante: Para instalar o com êxito o patch e o conector do CA Process Automation, encerre todos os nós do orquestrador e instale o patch e conector do CA Process Automation em todos os nós (domínio e não domínio).

Siga estas etapas:

1. Clique no executável do conector do CA Process Automation.

   A página de boas-vindas será exibida.

2. Aceite o contrato de licença e clique em Avançar.
3. Na página Selecione o diretório de instalação do CA Process Automation, forneça o local do *install_dir*.
4. Na página Escolher conectores a serem instalados/atualizados, selecione os conectores a serem instalados e clique em Avançar.

   O conector do CA Process Automation será instalado.

5. Para verificar a instalação do conector do CA Process Automation, vá até o CA Process Automation e efetue logon. Clique na guia Criador e clique em Novo processo.

   O conector do CA Process Automation instalado com seus operadores é listado na exibição de operadores.

Alterar a configuração do servidor de banco de dados Oracle para usar um Oracle RAC

É possível continuar a usar o servidor de banco de dados Oracle que você configurou para o CA Process Automation e que foi configurado durante a instalação do CA Process Automation. Se esse único servidor Oracle fizer parte de um Oracle RAC agrupado, você pode (opcionalmente) configurar o Oracle RAC como o servidor de banco de dados como uma tarefa pós-instalação.

Siga estas etapas:

1. Verifique se o CA Process Automation usa com êxito o único servidor de banco de dados Oracle configurado especificado durante a instalação do banco de dados da biblioteca, do banco de dados de tempo de execução e do banco de dados de relatórios.
2. Interrompa o serviço do CA Process Automation conforme descrito no tópico Interromper o orquestrador (na página 137).
3. Abra o arquivo OasisConfig.properties

   install_dir\server\c2o\.config\OasisConfig.properties
4. Modifique as seguintes entradas para o banco de dados da biblioteca:

   oasis.database.connectionurl=jdbc:oracle:thin:@//*oracle-server*:1521/
   oasis.database.lib.dbname=*ServiceName*
   oasis.database.queues.dbname=*ServiceName*
   oasis.database.dbhostname=*Oracle-RAC*
5. Modifique as seguintes entradas para o banco de dados de tempo de execução:

   oasis.runtime.database.connectionurl=jdbc:oracle:thin:@//*oracle-server*:1521/
   oasis.runtime.database.dbname=*ServiceName*
   oasis.runtime.database.dbhostname=*Oracle-RAC*
6. Modifique as seguintes entradas para o banco de dados de relatórios:

   oasis.reporting.database.connectionurl=jdbc:oracle:thin:@//*oracle-server*:1521/
   oasis.reporting.database.dbname=*ServiceName*
   oasis.reporting.database.dbhostname=*Oracle-RAC*
7. Salve o arquivo OasisConfig.properties.
8. Inicie o orquestrador (na página 138).

Observação: para as instruções do URL de conexão, as seguintes notações também são válidas:

Notação TNS

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=ora
cle-server)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=ServiceName)
))
```

Notação TNS RAC

```
jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=OFF)(FAILOVER=ON)(
ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-server)(PORT=1
521))(ADDRESS=(PROTOCOL=TCP)(HOST=oracle-server)(PORT=1521)))(C
ONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=ServiceName)))
```

Outra notação (sem barras de encaminhamento; instrução terminando com dois pontos)

```
jdbc:oracle:thin:@oracle-server:1521:
```

Interromper o orquestrador

Apenas administradores com credenciais de administrador no servidor onde o orquestrador está instalado podem interromper o orquestrador.

Importante: se um orquestrador não for desligado corretamente, a seguinte pasta temporária poderá acumular vários gigabytes de arquivos. Se isso acontecer, você pode excluir a pasta tmp com segurança:

install_dir/server/c2o/tmp

Siga estas etapas:

1. Usando credenciais de Administrador, efetue logon no host em que o Orquestrador de destino está instalado.
2. Se estiver conectado a um host do Windows, você pode interromper o serviço do orquestrador no menu Iniciar, na janela Serviços, ou na linha de comando. Realize uma da seguintes ações:
   - No menu Iniciar, selecione Programas, CA, CA Process Automation 4.0 e Interromper serviço do orquestrador.
   - Selecione Ferramentas Administrativas e Serviços no Painel de Controle. Selecione o seguinte serviço e clique em Interromper:

     Orquestrador do CA Process Automation (C:\Arquivos de Programas/CA/PAM/server/c2o)
   - Abra um prompt de comando e execute o seguinte script:

     install_dir/server/c2o/bin/stopc2osvc.bat
3. Se você estiver conectado a um host do UNIX ou Linux, execute as seguintes etapas:
   a. Altere os diretórios para ${PAM_HOME}/server/c2o/. Por exemplo, altere os diretórios para:

      /usr/local/CA/PAM/server/c2o
   b. Execute o script c2osvrd.sh com a opção stop. Por exemplo:

      ./c2osvrd.sh stop

Iniciar o orquestrador

Apenas administradores com credenciais de administrador no servidor onde o orquestrador está instalado podem reiniciar o serviço do orquestrador.

Siga estas etapas:

1. Usando as credenciais de administrador, efetue logon no host em que o orquestrador de destino está instalado.
2. Se estiver conectado a um host do Windows, você pode reiniciar o serviço do orquestrador no menu Iniciar, na janela Serviços, ou na linha de comando. Execute uma das tarefas a seguir:
   - Selecione Programas, CA, CA Process Automation e Iniciar serviço do orquestrador, no menu Iniciar.
   - Selecione Ferramentas Administrativas e Serviços no Painel de Controle. Selecione o seguinte serviço e clique em Iniciar:

     `Orquestrador do CA Process Automation (C:\Arquivos de Programas/CA/PAM/server/c2o)`
   - Abra um prompt de comando e execute o seguinte script:

     `install_dir``/server/c2o/bin/startc2osvc.bat`
3. Se você estiver conectado a um host do UNIX ou Linux, execute as seguintes tarefas:
   a. Altere os diretórios para ${PAM_HOME}/server/c2o/. Por exemplo, altere os diretórios para:

      `/usr/local/CA/PAM/server/c2o`
   b. Execute o script c2osvrd.sh com a opção start. Ou seja, execute:

      `./c2osvrd.sh start`

Observação: após iniciar o serviço para o orquestrador de domínio, inicie o CA Process Automation.

Desinstalar o orquestrador de domínio

Apenas administradores com credenciais de administrador no servidor onde o orquestrador de domínio está instalado podem desinstalá-lo.

Observação: interrompa o orquestrador de domínio antes de desinstalá-lo.

Siga estas etapas:

1. Usando credenciais de Administrador, efetue logon no host em que o orquestrador de domínio de destino está instalado.
2. Se você efetuou logon nos seguintes hosts:
   a. Um host do Windows:
   Você pode desinstalar o orquestrador de domínio no menu Iniciar, Painel de Controle. Execute uma das seguintes tarefas:
      - Selecione Programas, CA, CA Process Automation 4.2 e Desinstalar CA Process Automation no menu Iniciar.
      - Selecione a entrada do domínio do CA Process Automation no menu Iniciar, Painel de Controle, Programas e Recursos e clique em Desinstalar.

        O assistente de desinstalação será exibido.

   b. Para um host do UNIX ou Linux, execute as seguintes tarefas:
      a. Mude para o diretório ${PAM_HOME}/standalone/. Por exemplo, altere os diretórios para:

         `/usr/local/CA/PAM/server/c2o`

      b. Execute o script ./uninstall.

         O assistente de desinstalação será exibido.
3. Depois que o orquestrador de domínio for desinstalado, verifique as seguintes alterações:
   - Em Ferramentas Administrativas e Serviços no Painel de Controle, o serviço do domínio do CA Process Automation será excluído.
   - A entrada do domínio do CA Process Automation será removida do menu Iniciar, Painel de Controle, Programas e Recursos.
   - A pasta do orquestrador de domínio será removida do local de instalação.

Capítulo 6: Atualizar para a release atual

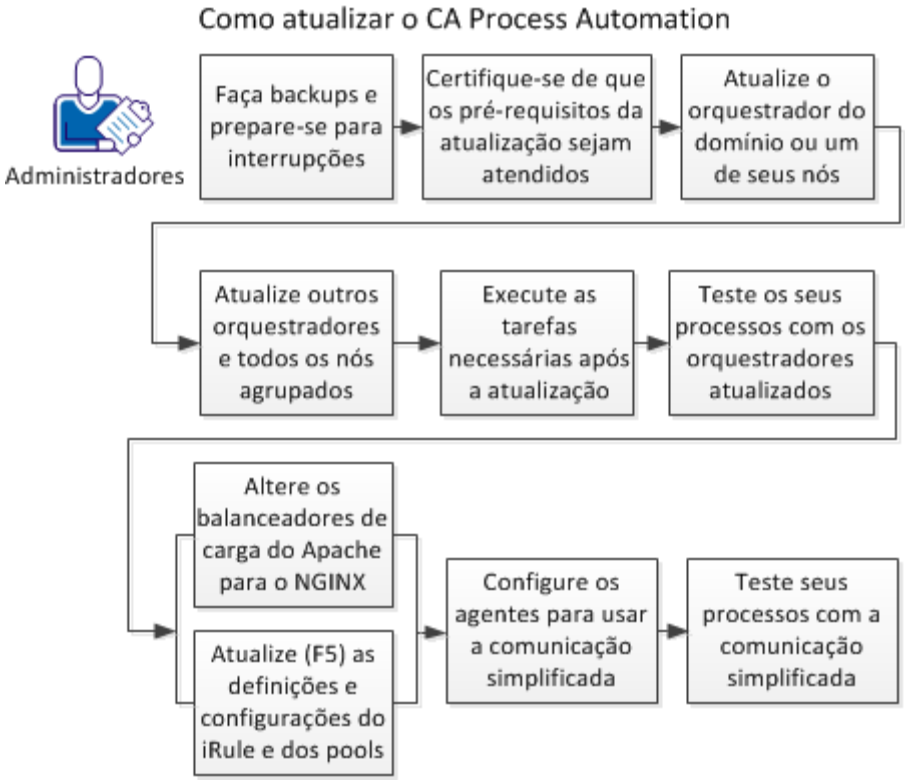
É possível atualizar para o CA Process Automation Release 4.2 a partir das seguintes versões do CA Process Automation:

- CA Process Automation 3.1 SP01
- CA Process Automation 4.0 SP01
- CA Process Automation Release 4.1
- CA Process Automation 4.1 SP01

Esta seção contém os seguintes tópicos:

Como atualizar o CA Process Automation

É possível atualizar para o CA Process Automation Release 4.2 a partir da release 3.1 SP01 e acima usando o processo ilustrado.



Importante: Se necessário, atualizar de uma release anterior para a r3.1 SP01 (na página 292) antes de começar o processo documentado aqui.

Siga estas etapas:

1. Fazer backups e preparar para a interrupção (na página 143).
2. Executar os pré-requisitos de atualização (na página 144).
3. Atualizar o orquestrador de domínio (na página 146).
4. Atualizar outros orquestradores e todos os nós agrupados.
   - Atualizar um orquestrador não agrupado (na página 149).
   - Atualizar um nó de agrupamento (na página 152).
5. Executar tarefas pós-atualização (na página 155).
6. Testar os processos com os orquestradores atualizados (na página 156).
7. Um dos seguintes:
   - Alternar os balanceadores de carga do Apache para o NGINX (na página 157).
   - Atualizar os pools do F5, a definição da iRule e a configuração (na página 157).
8. Configurar os agentes para usarem a comunicação simplificada (na página 158).
9. Testar os processos com a comunicação simplificada (na página 159).

Fazer backups e preparar para a interrupção

Incidentes inesperados ou incontroláveis podem interromper ou, de alguma forma, fazer com que o processo de atualização falhe. Por precaução, é recomendável fazer backup de todos os dados importantes armazenados em pastas do CA Process Automation antes de começar a atualização. Para se preparar para a reversão total, também faça backup do conteúdo do CA Process Automation que você armazena nos servidores de banco de dados e no CA EEM.

Siga estas etapas:

1. Verifique se os servidores de banco de dados têm acesso a pelo menos o dobro de espaço que está sendo usado no momento pelos bancos de dados do CA Process Automation existentes.
2. Para se preparar para uma reversão em potencial, faça um instantâneo de todas as VM do orquestrador ou faça backup da seguinte pasta em todos os orquestradores:

   `install_dir/server/c2o/`

   A prática recomendada é fazer backup dessa pasta em um disco físico diferente daquele que hospeda a pasta *install_dir*.
3. Faça backup do armazenamento de dados de relatórios, de tempo de execução e da biblioteca usados por cada orquestrador antes da atualização. Os armazenamentos de dados podem residir em diferentes servidores de banco de dados ou todos no mesmo servidor de banco de dados.

4. Faça backup do aplicativo do CA Process Automation no seu servidor do CA EEM.
   a. Efetue logon no CA EEM, especificando o aplicativo CA Process Automation.
   b. Clique na guia Configurar, clique em Servidor do EEM e clique em Exportar aplicativo.
   c. Clique em Exportar e salve o arquivo <nome-do-aplicativo>.gz na unidade local.
5. Preparar para uma interrupção. A duração da atualização de um orquestrador depende do tamanho dos armazenamentos de dados. Quanto mais dados houver, mais tempo levará a atualização.
   - Se houver outros aplicativos que dependem dos serviços do CA Process Automation, prepare para essa interrupção. Por exemplo, se usar o Service Catalog para iniciar processos do CA Process Automation, você pode encerrar o Service Catalog durante a atualização do CA Process Automation. Como alternativa, é possível apresentar uma caixa de diálogo de "temporariamente indisponível" para os itens de catálogo que dependem do CA Process Automation e, em seguida, remover essa caixa de diálogo quando a atualização do CA Process Automation estiver concluída.
   - Programe uma janela de manutenção apropriada e informe aos stakeholders relevantes sobre o intervalo de tempo em que se espera que o CA Process Automation esteja indisponível.

Executar os pré-requisitos de atualização

Antes de iniciar o processo de atualização para o CA Process Automation Release 04.2.00, execute as seguintes tarefas de pré-requisito:

1. Tenha à mão as credenciais do administrador do CA EEM, onde EiamAdmin é normalmente o Nome de usuário do administrador do EEM e a Senha do admin do EEM é conhecida para o administrador do CA EEM.
2. Registre a senha do certificado a ser usada para esta atualização do sistema.

   A senha do certificado é usada para controlar o acesso às chaves usadas para criptografar senhas e outros dados críticos. Especifique essa senha para o primeiro orquestrador que você atualizar. Em seguida, você deve digitar essa mesma senha ao instalar outros nós do orquestrador de domínio, outros orquestradores autônomos e nós de outros orquestradores agrupados para a mesma release.

   Importante: Você deve usar a mesma senha do certificado que foi usada com a release a partir da qual está atualizando.
3. Certifique-se de que não há processos do CA Process Automation ativos no momento, ou seja, no estado Em execução ou no estado Bloqueado.
4. Encerre todos os orquestradores que não sejam de domínio. Para os orquestradores agrupados que não sejam de domínio, encerre o serviço do orquestrador em cada nó. Consulte o tópico Interromper o orquestrador (na página 137).

5. Encerre o orquestrador de domínio. Para um orquestrador de domínio agrupado, encerre o serviço do orquestrador em cada nó. Consulte o tópico Interromper o orquestrador (na página 137).

   Observações:

   - Os agentes ativos não conseguem estabelecer conexão com os orquestradores encerrados, mas irão se reconectar quando os orquestradores forem reiniciados.
   - Os processos e operadores programados não serão executados durante o processo de atualização.

6. Se você usar um balanceador de carga do Apache, copie os modelos de configuração do Apache atualizado do DVD1. Para obter detalhes, consulte o tópico Balanceador de carga do Apache (na página 257).

7. Se você usar um balanceador de carga F5, atualize a definição da iRule para remover a designação de nó principal. Essa alteração permite continuar a usar a comunicação obsoleta para a primeira fase da atualização.

   a. Remover: set PRIMARY "[PrimaryIP]"

   b. Remover: set PRIMPORT "[PrimaryPort]"

   c. Remover todas as ocorrências: member $PRIMARY $PRIMPORT

8. Verifique se a versão do JDK instalada em todos os nós do orquestrador é uma versão suportada. Consulte o tópico Pré-requisitos do JDK (na página 76).

9. Se o nome do host DNS definido ao instalar o CA Process Automation contiver caracteres restritos (como sublinhados), corrija o nome do host DNS. Para obter mais informações, consulte Resolver caractere inválido no nome DNS do CA Process Automation (na página 244).

10. Verifique se o CA EEM está em execução.

    Observação: se estiver usando um servidor LDAP diferente do CA Embedded Entitlements Manager (CA EEM), instale o CA EEM agora e inicie-o. (O CA EEM é o único servidor de diretório que é suportado pelo CA Process Automation 4.0 e posterior.)

11. Atualize todos os conectores do CA Process Automation que não sejam conectores 4.x.

Atualizar o orquestrador de domínio

É possível atualizar diretamente para o CA Process Automation Release 4.2 a partir das seguintes versões do CA Process Automation:

- CA Process Automation Service Pack 3.1sp01
- CA Process Automation Service Pack 4.0sp01
- CA Process Automation Release 4.1
- CA Process Automation Service Pack 4.1sp01

Siga estas etapas:

1. Efetue logon no host em que o orquestrador de domínio (ou um nó do orquestrador de domínio) está instalado.
2. Navegue até a pasta DVD1 da mídia de instalação e inicie o assistente de instalação a partir do arquivo do seu sistema operacional:
   - **Windows:** Domain_Installer_windows.bat
   - **Linux ou UNIX**: Domain_Installer_unix.sh

   Esses arquivos chamam o instalador de terceiros e, em seguida, o instalador do orquestrador de domínio.
3. Clique em Avançar para percorrer as páginas iniciais do assistente:
   - Idioma
   - Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation
   - Contrato de licença - Eu aceito os termos do Contrato de Licença
   - Selecionar o diretório de destino
   - Pré-requisitos para a instalação do CA Process Automation
4. A Instalação do JDBC Jars é exibida,
   - Clique em Avançar se você usa o Oracle como servidor de banco de dados.
   - Clique em Adicionar arquivos, se você usa o MySQL ou o SQL Server como servidor de banco de dados.
     - Se você usa o MySQL, vá até o local em que fez download do arquivo JAR apropriado.
     - Se você usa o SQL Server, vá até o ...DVD1\drivers\jtds-1.3.jar.
5. Clique em Avançar para obter os pré-requisitos para instalação do CA Process Automation.

6. Quando Concluindo o Assistente de instalação do CA Process Automation é exibido, substitua DVD1 por DVD2 no caminho do diretório. Em seguida, clique em Concluir.

   A mensagem será exibida: "Copiando o instalador do CA Process Automation. Isso pode levar alguns minutos. Aguarde." Talvez haja um tempo de atraso entre o fechamento dessa página e a abertura da página de boas-vindas.

7. Quando Bem-vindo ao Assistente de instalação de domínio do CA Process Automation é exibido, clique nas páginas iniciais do assistente:

   - Idioma
   - Bem-vindo ao Assistente de instalação de domínio do CA Process Automation
   - Contrato de licença - Eu aceito os termos do Contrato de Licença

8. Verifique se o Diretório inicial do Java aponta para a versão de JDK suportada por esta release.

9. Continue clicando por meio das páginas:

   - Reinstalar
   - Tela de configuração

10. Quando Definir senha do certificado é exibido, digite a senha que foi especificada durante a instalação da última release. Registre a senha para referência futura, pois você precisará dessa senha para atualizar todos os outros orquestradores e os nós do orquestrador neste domínio do CA Process Automation. Clique em Avançar.

11. Clique em selecionar a pasta do menu Iniciar para usar a seleção anterior.

12. Na página Propriedades gerais, observe as seguintes alterações nos padrões da porta do servidor do orquestrador:

    Porta do servidor

    Define a porta que o orquestrador de domínio usa para se comunicar com outros orquestradores e agentes. Essa porta é usada pela comunicação simplificada.

    Padrão: 80 (básico: HTTP) ou 443 (protegido: HTTPS)

    Porta do servidor obsoleta

    O valor da Porta do servidor que foi definido para uma release anterior do CA Process Automation. Essa porta é usada pela comunicação obsoleta.

    Padrão: 7001

13. Clique nas páginas a seguir, fazendo alterações a seu critério.

    - Diretório temporário de scripts
    - Diretiva de execução do PowerShell

14. Quando Configurações de Segurança do EEM (Embedded Entitlements Manager) é exibido,
    a. Selecione Registrar o aplicativo com o CA EEM e clique em Registrar.
    b. Forneça credenciais para efetuar logon no CA EEM como o administrador EiamAdmin.
    c. Concorde com a atualização. O processo de instalação detecta a versão do servidor do CA EEM e escolhe o SDK apropriado.
    d. Clique em OK quando a confirmação de aplicativo registrado for exibida.
15. Clique nas Configurações do banco de dados, pois você já as definiu:
    - Banco de dados do repositório
    - Banco de dados de tempo de execução
    - Banco de dados de relatórios
16. Clique em Jars adicionais para instalação se não há nada a ser adicionado.
17. Quando Concluindo o Assistente de instalação de domínio do CA Process Automation é exibido, clique em Concluir.

    Importante: Um tempo significativo é necessário para que o orquestrador de domínio se torne disponível para logon. A atualização de orquestradores adicionais ou de nós adicionais, se o orquestrador de domínio estiver agrupado, pode iniciar apenas depois que se possa efetuar logon no orquestrador de domínio.
18. Inicie o serviço do orquestrador no orquestrador de domínio.

    Observação: consulte o tópico Iniciar orquestradores (na página 138) para obter os detalhes específicos do sistema operacional.

Tarefas de atualização adicionais (após a conclusão do Assistente de instalação de domínio)

1. Considere fazer o ajuste do JVM atualizando os valores em *install_dir*/server/c2o/bin/c2osvcw.conf. Por exemplo:

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Os valores wrapper.java.initmemory e wrapper.java.maxmemory devem ser idênticos. Se for necessário memória adicional e estiver disponível no servidor, esses valores podem ser alterados. Depois de alterar quaisquer valores de configuração, reinicie o serviço do CA Process Automation.

2. Considere atualizar os valores padrão de JBOSS JMS e de pools de banco de dados em *install_dir*/server/c2o/conf/standardjboss.xml. Por exemplo:

   - Em <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cach
     e-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Em <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

3. Se estiver usando o CA EEM 12.51 com o CA Process Automation atualizado e o CA EEM configurado para fazer referência a vários Microsoft Active Directories ou a uma floresta do AD, recrie os usuários do CA Process Automation no CA EEM.

   Observação: consulte "Gerenciar o acesso para contas de usuários referenciadas" no *Guia de Administrador de Conteúdo*.

Mais informações:

Considerações sobre atualização (instalação silenciosa) (na página 123)

Atualizar um orquestrador não agrupado

Depois de atualizar o orquestrador de domínio chamando um script distribuído na mídia, é possível atualizar outros orquestradores por meio da interface de usuário do CA Process Automation.

Siga estas etapas:

1. Efetue logon no host com o orquestrador a ser atualizado.
2. Navegue até o CA Process Automation e efetue logon (na página 173) com as credenciais de administrador.
3. Clique na guia Configuração e selecione a paleta Instalação.
4. Clique em Instalar na seção Instalar orquestrador para iniciar a atualização.
5. Selecione um idioma e clique em OK.

   A página Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation é exibida.

6. Clique em Avançar para prosseguir com as seguintes páginas do assistente de instalação:
   - Contrato de Licença - Selecione a opção para aceitar o contrato.
   - Diretório de instalação padrão
   - Pré-requisitos para a instalação do CA Process Automation
7. Especifique o jars do JDBC para instalação de uma das seguintes maneiras:
   - Deixe a caixa de seleção Usar domínio selecionada e clique em Avançar. Isso especifica o uso dos JDBC Jars que a instalação do orquestrador de domínio configurou.
   - Conclua o seguinte procedimento:
     a. Desmarque a caixa de seleção Usar domínio.
     b. Clique em Adicionar arquivos.
     c. Selecione o tipo de servidor de banco de dados.
     d. Clique em Procurar e navegue até o arquivo JDBC JAR do tipo de servidor selecionado.
     e. Clique em Avançar.
8. Clique em Avançar para confirmar e, em seguida, clique em Concluir para prosseguir para o instalador do CA Process Automation.
9. Clique em Avançar na página de boas-vindas
10. Selecione a opção para aceitar o contrato de licença e clique em Avançar.
11. Quando a página do Diretório inicial do Java é exibida, vá até o local do JDK atualizado e, em seguida, clique em Avançar.
12. Clique em Avançar para prosseguir com as seguintes páginas do assistente de instalação:
    - URL do domínio
    - Página do balanceador de carga e Single Sign On
    - nome da empresa:
13. Digitar a senha do certificado e clicar em Avançar.

    Essa senha do certificado é a mesma que o orquestrador de domínio usa. Digite a mesma senha do certificado que foi inserida quando o orquestrador de domínio foi instalado. Essa também é a mesma senha do certificado usada na release a partir da qual você está atualizando.

14. Clique em Avançar para aceitar a configuração anterior nas seguintes páginas do assistente de instalação:
    - Preferências da pasta do menu Iniciar e clique em Avançar.
    - Propriedades gerais
    - Diretório temporário de scripts
    - Diretiva de execução do PowerShell
    - Configurações do banco de dados do repositório para esse orquestrador
    - Configurações do banco de dados de tempo de execução
    - Configurações do banco de dados de relatórios
15. Clique em Concluir.
16. Quando o processamento estiver concluído, inicie o serviço do orquestrador no orquestrador não agrupado atualizado.

    Observação: consulte o tópico Iniciar orquestradores (na página 138) para obter os detalhes específicos do sistema operacional.

Tarefas de atualização adicionais

1. Considere fazer o ajuste do JVM atualizando os valores em *install_dir*/server/c2o/bin/c2osvcw.conf. Por exemplo:

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Os valores wrapper.java.initmemory e wrapper.java.maxmemory devem ser idênticos. Se for necessário memória adicional e estiver disponível no servidor, esses valores podem ser alterados.

2. Considere atualizar os valores padrão de JBOSS JMS e de pools de banco de dados em *install_dir*/server/c2o/conf/standardjboss.xml. Por exemplo:
   - Em <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cache-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Em <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

mais informações:

Exemplo: atualizar um orquestrador não agrupado da Release 4.1 SP01 para a 4.2 no Windows (na página 286)

Atualizar um nó de agrupamento

Ao atualizar um orquestrador agrupado, atualize um nó de cada vez, começando com qualquer nó no agrupamento.

Siga estas etapas:

1. Efetue logon no host em que um nó de agrupamento esteja instalado.
2. Vá até o URL do orquestrador de domínio (o balanceador de carga do orquestrador de domínio, se agrupado).
3. Efetue logon, clique na guia Configuração e, em seguida, clique na paleta Instalação.
4. Em Instalar o nó de agrupamento do orquestrador, clique em Instalar para iniciar a atualização.
5. A caixa de diálogo de seleção de idioma é exibida em primeiro lugar. Clique em OK.
6. Clique nas páginas seguintes do assistente:
   - Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation.
   - Contrato de Licença - selecione Eu aceito os termos do Contrato de Licença
   - Selecione o diretório de destino, C:\Arquivos de Programas\CA\PAM, por padrão.
   - Pré-requisitos para instalação do CA Process Automation - chama a instalação.
   - Concluindo o Assistente de instalação do CA Process Automation com a opção Usar domínio selecionada - Clique em Concluir

     Aguarde até que a próxima página seja exibida. Não há nenhum indicador visual do processamento que preceda a exibição da próxima página.
   - Bem-vindo ao Assistente de instalação de domínio do CA Process Automation
   - Contrato de licença
7. Se você atualizou o JDK, vá até o Diretório inicial do Java, por exemplo, C:\Arquivos de Programas\Java\jdk1.7.0_45

8. Preencha a Tela de configuração:
   a. Se já tiver atualizado um nó nesse agrupamento, selecione na lista suspensa Orquestrador o nó do orquestrador que foi atualizado primeiro.
   b. Digite node1, node2, node3 ou node4 no campo Nó de funcionário do balanceador de carga para identificar o nó que está sendo atualizado.
9. Digite o nome da sua empresa, caso não seja exibido
10. Digite a sua senha do certificado.

    Importante: Essa entrada deve corresponder à senha do certificado que foi inserida quando o orquestrador de domínio foi atualizado.
11. Clique nas páginas seguintes, se forem exibidas. As configurações usadas pelo node1 são usadas por outros nós no agrupamento.
    - Selecione a pasta do menu Iniciar.
    - Página Propriedades gerais (Instalar como um serviço do Windows não é mostrado, mas é suposto).
    - Diretório temporário de scripts
    - PowerShell
    - Configurações de segurança do CA Embedded Entitlements Manager (CA EEM)
    - Configurações do banco de dados - Repositório
    - Configurações do banco de dados - Tempo de execução
    - Configurações do banco de dados - Relatórios

    A instalação de atualização é iniciada.
12. Quando a página Concluindo o Assistente de instalação do CA Process Automation for exibida, clique em Concluir.

    O processamento continua depois que você clica em Concluir.
13. Quando o processamento estiver concluído, inicie o serviço do orquestrador no nó de agrupamento atualizado.

    Observação: consulte o tópico Iniciar orquestradores (na página 138) para obter os detalhes específicos do sistema operacional.

Tarefas de atualização adicionais

1. Considere fazer o ajuste do JVM atualizando os valores em *install_dir*/server/c2o/bin/c2osvcw.conf. Por exemplo:

   ```
   wrapper.java.additional.7=-XX:PermSize=256m
   wrapper.java.additional.8=-XX:MaxPermSize=768m
   wrapper.java.initmemory=4096
   wrapper.java.maxmemory=4096
   ```

   Os valores wrapper.java.initmemory e wrapper.java.maxmemory devem ser idênticos. Se for necessário memória adicional e estiver disponível no servidor, esses valores podem ser alterados.

2. Considere atualizar os valores padrão de JBOSS JMS e de pools de banco de dados em *install_dir*/server/c2o/conf/standardjboss.xml. Por exemplo:

   - Em <jndi-name> DefaultDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <prepared-statement-cache-size>250</prepared-statement-cache-size>
     <max-pool-size>375</max-pool-size>
     ```

   - Em <jndi-name> DDLDatasourceDS</jndi-name>

     ```
     <idle-timeout-minutes>10</idle-timeout-minutes>
     <max-pool-size>375</max-pool-size>
     ```

Mais informações:

Exemplo: atualizar qualquer nó do orquestrador de domínio da Release 3.1 SP01 para a 4.2 no Windows (na página 277)
Exemplo: atualizar outro nó do orquestrador de domínio da Release 3.1 SP01 para a 4.2 no Windows (na página 283)

Executar tarefas pós-atualização

Após atualizar para o CA Process Automation Release 4.2, execute as seguintes tarefas pós-atualização:

1. Executar encaminhamento de modificações do arquivo de configuração.
   a. Vá até o seguinte local de backup:

      `install_dir/config_backup_MM_dd_yyyy_HHmm`

   b. Use uma ferramenta de comparação de arquivos para realçar as diferenças entre os seguintes arquivos de configuração cujo backup foi feito e a versão atual do CA Process Automation.
      `install_dir/server/c2o/.config/OasisConfig.properties`
      `install_dir/server/c2o/bin/c2osvcw.conf`
      `install_dir/server/c2o/conf/standardjboss.xml`
      `install_dir/server/c2o/conf/log4j.xml`

   c. Aplique as alterações apropriadas na versão atual do CA Process Automation.
2. Navegue para o CA Process Automation e efetue logon (na página 173).
3. Clique na guia Configuração e examine o Navegador de configuração.
4. Verifique se todos os orquestradores aparecem sob o nó Orquestradores e se os touchpoints associados do orquestrador aparecem na hierarquia de domínio no ambiente correto. Se qualquer orquestrador não estiver ativo, inicie o orquestrador (na página 138).
5. Verifique se os agentes foram reiniciados. Agentes que usam a comunicação obsoleta reiniciam automaticamente. Se algum agente estiver encerrado, inicie-o como descrito em Iniciar um agente (na página 182).
6. Se estiver usando o CA EEM 12.51 com o CA Process Automation atualizado e o CA EEM configurado para fazer referência a vários Microsoft Active Directories ou a uma floresta do AD, recrie a propriedade do objeto.

   Observação: consulte o tópico "Alterar a propriedade de um objeto de automação" no *Guia do Criador de Conteúdo*.

Testar os processos com os orquestradores atualizados

Depois de concluir a atualização, teste seus processos com o CA Process Automation atualizado. Considere a abordagem a seguir. Verifique se os processos são executados com êxito em todos os orquestradores.

Siga estas etapas:

1. Inicie um processo que gera uma tarefa. Selecione a tarefa para si mesmo. Verifique se a instância do processo aparece na guia Início. Verifique se a tarefa que você selecionou é exibida na Lista de tarefas.
2. Inicie um processo ou um operador programado. Verifique se ele é iniciado na hora certa e se é concluído com êxito.
3. Inicie um processo com os operadores que são executados em touchpoints do agente ou em hosts remotos por meio de touchpoints do proxy. Verifique se a instância do processo é concluída com êxito.
4. Permita que as soluções que usam o CA Process Automation como um componente integrado sejam executadas. Monitore os resultados e verifique se nada inesperado ocorre.

Alternar os balanceadores de carga do Apache para o NGINX

Se você tiver usado um balanceador de carga do Apache para os orquestradores agrupados antes da atualização, é recomendável manter esse balanceador de carga até que tenha verificado que tudo está funcionando sem problemas com a nova release. Isso exige que você atualize a configuração do Apache com novos modelos fornecidos na mídia de instalação.

A alteração para o NGINX após uma atualização não é diferente da configuração do NGINX em uma nova release, exceto pelo fato de que em atualizações, instala-se o NGINX no mesmo servidor em que o balanceador de carga do Apache existente atualmente. Isso permite aproveitar o URL estabelecido anteriormente e as portas e nomes de host estabelecidos anteriormente.

Para obter detalhes sobre a configuração, consulte o tópico Balanceador de carga NGINX (na página 35).

Os agentes se comunicam com os orquestradores; os orquestradores se comunicam com os agentes. A Release 4.2 apresenta um método melhorado de comunicação simplificada. O Apache usa o método de comunicação obsoleta. Por padrão, os agentes existentes são configurados para usar a comunicação obsoleta. Essa configuração padrão permite alternar os balanceadores de carga do Apache para o NGINX e converter os agentes existentes para usar a comunicação simplificada em um momento conveniente depois da conclusão das tarefas obrigatórias de atualização. O NGINX oferece suporte à comunicação simplificada. (O NGINX também oferece suporte à comunicação obsoleta.)

Atualizar os pools do F5, a definição da iRule e a configuração

Para usar a comunicação simplificada, modifique a configuração do F5.

Siga estas etapas:

1. Criar dois pools do F5 para cada agrupamento do CA Process Automation. (na página 55)
2. Substituir a iRule atual pela definição da iRule (na página 58).
3. Configurar o F5 para usar a comunicação simplificada com HTTPS (na página 61).

Configurar o agente para usar a comunicação simplificada

É necessário reinstalar os agentes existentes para alternar a comunicação do agente da comunicação obsoleta para a simplificada. Isto pode ser feito para todos os agentes depois de atualizar para o CA Process Automation 04.2.00 e instalar e configurar um balanceador de carga NGINX.

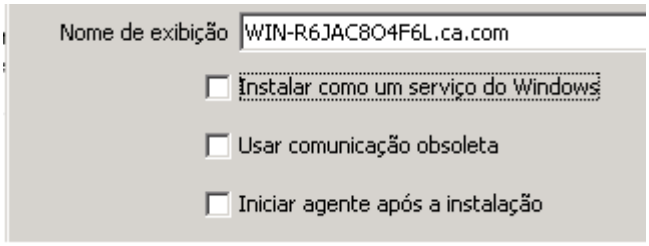
Reinstale cada agente conforme descrito no tópico Instalar um agente de forma interativa (na página 174). Por padrão, a caixa de seleção Usar comunicação obsoleta está desmarcada. Deixar esta caixa de seleção desmarcada, instala o agente para usar a comunicação simplificada.

O agente cria conexões de soquete da web e envia os detalhes da conexão para todos os nós do orquestrador. Os orquestradores usam a conexão de soquete da web para enviar solicitações ou atualizações para o agente, conforme necessário.

Sobre a comunicação do agente

Você configura as comunicações do agente ao instalar um agente. Por padrão, os novos agentes usam a comunicação simplificada (a caixa de seleção Usar comunicação obsoleta está desmarcada).

Os agentes atualizados usam a comunicação obsoleta. É possível reconfigurar essa configuração sem reinstalar o agente.



Comunicação simplificada

A comunicação simplificada usa soquetes da web e o HTTP para produzir uma conexão persistente em uma única via, do agente para o orquestrador. O CA Process Automation usa uma porta padrão (80 ou 443) que fornece uma conexão rápida entre os componentes.

Comunicação obsoleta

A comunicação obsoleta, que usa várias portas, não é tão amigável com o firewall ou com um roteador NAT quanto a comunicação simplificada. As conexões iniciadas pelo orquestrador usadas na comunicação obsoleta não são tão eficazes quanto as conexões persistentes usadas na comunicação simplificada.

Mais informações

Portas usadas pelo balanceador de carga (na página 227)

Testar os processos com a comunicação simplificada

Depois de configurar o balanceador de carga NGINX para cada orquestrador agrupado, teste os processos novamente. Considere a abordagem a seguir. Verifique se os processos são executados com êxito em todos os orquestradores.

Siga estas etapas:

1. Inicie um processo que gera uma tarefa. Selecione a tarefa para si mesmo. Verifique se a instância do processo aparece na guia Início. Verifique se a tarefa que você selecionou é exibida na Lista de tarefas.
2. Inicie um processo ou um operador programado. Verifique se ele é iniciado na hora certa e se é concluído com êxito.
3. Inicie um processo com os operadores que são executados em touchpoints do agente ou em hosts remotos por meio de touchpoints do proxy. Verifique se a instância do processo é concluída com êxito.
4. Permita que as soluções que usam o CA Process Automation como um componente integrado sejam executadas. Monitore os resultados e verifique se nada inesperado ocorre.
5. Quando estiver certo de que a nova release do CA Process Automation que opera com comunicações simplificadas está funcionando conforme o esperado, retome todo o processamento normal.

Capítulo 7: Reinstalar ou configurar a release atual

É possível fazer alterações na versão da release do orquestrador atual executando novamente o assistente de instalação. As opções incluem "Reinstalar" e "Configurar a instalação existente".

Esta seção contém os seguintes tópicos:

Exemplo de cenário: configurar a instalação existente para gerar novamente os certificados do CA Process Automation

Ao executar o processo de instalação para a release previamente instalada, você tem a opção de reinstalar ou configurar a instalação existente. Esse cenário de exemplo mostra como usar a opção de instalação configurada e existente para gerar novamente os certificados que o CA Process Automation usa para se conectar ao CA EEM.

O processo de instalação do orquestrador de domínio permite registrar (ou registrar novamente) o CA Process Automation com o CA EEM. Esse processo de registro irá gerar certificados de aplicativo para o CA Process Automation com o mesmo comprimento de chave que os certificados usados pelo CA EEM.

Observação: o CA Process Automation possui outros certificados que não são afetados pelo registro; o registro gera apenas os certificados que o CA Process Automation usa para se conectar ao CA EEM. O local do certificado é *install_dir*/server/c2o/.c2orepository/public/certification.

Esse cenário de exemplo adota a seguinte configuração:

1. O administrador do CA EEM instala ou atualiza para o CA EEM Release 12.51 com certificados padrão, que têm chaves de 1024 bits.
2. Instale ou atualize para o CA Process Automation Release 4.2. Os certificados do CA Process Automation gerados também possuem chaves de 1024 bits.
3. Posteriormente, o administrador do CA EEM gera certificados do CA EEM com comprimentos de chave mais longos (2048 bits ou 4096 bits).

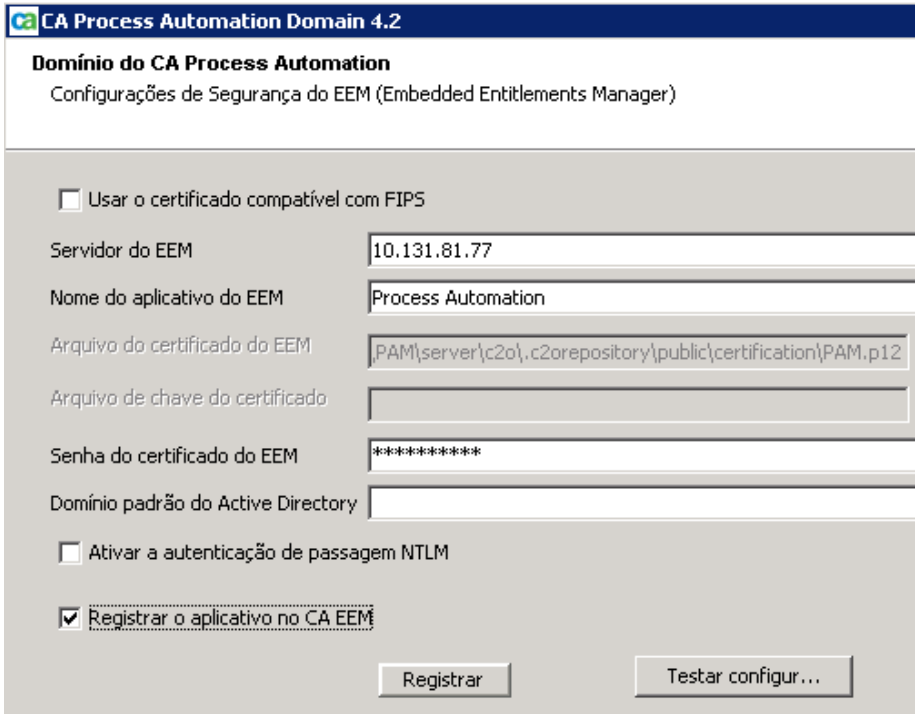
Nesse caso, use o procedimento a seguir para gerar certificados do CA Process Automation com comprimentos de chave que correspondam aos dos certificados do CA EEM.

Siga estas etapas:

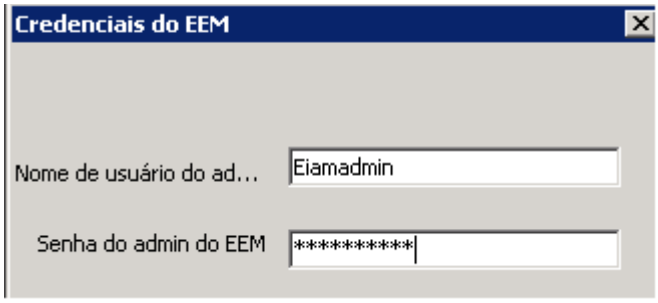
1. Instalar o software de terceiros (na página 93).

   Quando a instalação do software de terceiros for concluída, o processo de instalação do domínio do CA Process Automation começará.
2. Clique nas páginas iniciais até que a página Reinstalar/configurar seja exibida.
3. Selecione a opção Configurar instalação existente. (Esse processo modifica os arquivos de propriedades, mas não modifica nenhum JAR.)

4. Clique nas páginas até que a página Configurações de Segurança do EEM (Embedded Entitlements Manager) seja exibida.
5. Marque a caixa de seleção Registrar o aplicativo no CA EEM e, em seguida, clique em Registrar.

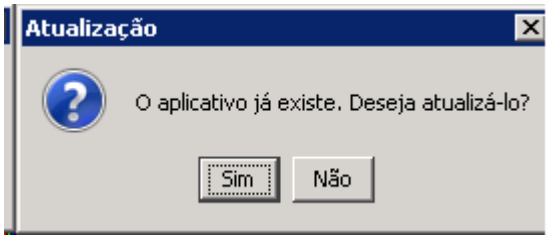


6. Digite as credenciais do administrador do CA EEM. Digite **EiamAdmin** em Nome de usuário do administrador do EEM. Digite a senha associada.



7. Clique em Sim para atualizar o aplicativo, mesmo que você não esteja atualizando a release do CA Process Automation.

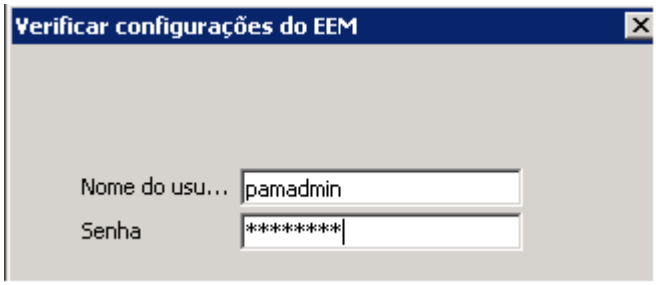
   (Clicar em Sim é necessário para a geração dos certificados de aplicativo que o CA Process Automation precisa.)



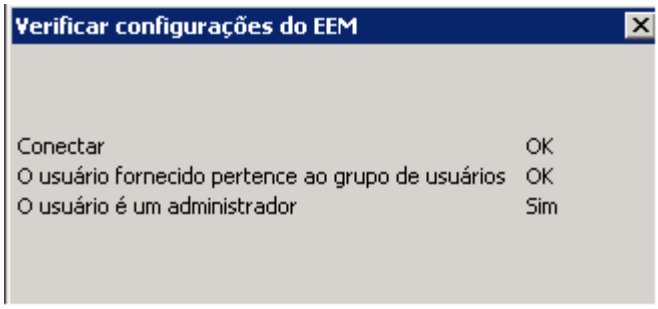
8. Clique em Testar configurações do EEM. Clique em OK para a configuração de mensagens.

9. Digite as credenciais de um usuário do CA Process Automation que está atribuído ao grupo PAMAdmins.

   Observação: o exemplo de entrada de **pamadmin**, **pamadmin**, é válido somente **se** você tiver configurado o CA EEM para usar o armazenamento de usuários interno.



10. Verifique se o CA Process Automation se conecte ao CA EEM e se o CA EEM autentica as credenciais.



11. Clique no restante do processo de instalação e, em seguida, clique em Concluir.

Suporte pós-instalação para atualizações do CA EEM

Se você estiver executando o processo de instalação com a mesma versão do CA Process Automation, serão exibidas as seguintes opções:

Reinstalar

Exibe todo o assistente de instalação.

Selecione a opção Reinstalar se sua instalação anterior usava o servidor do CA EEM Release 8.4, mas você tiver atualizado o servidor do CA EEM para a Release 12.

- Se registrar o aplicativo com o CA EEM Release 12.x, o processamento de reinstalação selecionará a versão principal 12 SDK do CA EEM.
- Caso você não registre o aplicativo, o processo de reinstalação solicitará que você selecione um SDK de acordo com sua versão do CA EEM.

Selecione a opção Reinstalar se você usar o CA EEM Release 12.5, mas a versão do SDK for a versão principal 8. O processo de reinstalação atualiza o SDK para a versão principal 12.

Observação: o CA Process Automation pode usar a versão principal 8 do CA EEM SDK com o CA EEM Release 12.x. Atualizar o SDK para a versão principal 12 permite usar os novos recursos do CA EEM.

Configurar a instalação existente

Exibe apenas páginas selecionadas. (Esse processo modifica os arquivos de propriedades, mas não modifica nenhum JAR.)

Selecione esta opção se você tiver gerado certificados do CA EEM com comprimentos de chave mais longos (2048 ou 4096) depois de instalar ou atualizar o CA Process Automation para a Release 4.2.

Quando você clicar na opção Registrar na página de configuração do CA EEM, o CA Process Automation perguntará se você deseja atualizar o aplicativo existente no CA EEM. Quando você aceitar a atualização, certificados do CA Process Automation (usados para se comunicar com o CA EEM) serão gerados novamente. Os novos certificados do CA Process Automation possuem comprimentos de chave que correspondem aos cumprimentos dos certificados do CA EEM.

Observação: consulte a documentação do CA EEM para obter mais informações sobre como atualizar o CA EEM ou seus certificados.

O CA Process Automation usa o CA EEM SDK para se comunicar com o CA EEM; a comunicação é protegida com certificados. O CA EEM e o CA Process Automation têm certificados. Os certificados do CA Process Automation devem ter o mesmo comprimento de chave que os certificados do CA EEM.

Durante a instalação do CA Process Automation Release 4.2 ou a atualização para a Release 4.2, o processo de instalação recupera os certificados do CA Process Automation do CA EEM e escolhe o SDK apropriado para o CA EEM associado. Esses certificados podem ser encontradas aqui:

install_dir/server/c2o/.c2orepository/public/certification

Desde que o CA EEM não seja alterado, nenhuma ação é necessária. No entanto, as seguintes alterações no CA EEM exigem sua ação.

Instale o CA Process Automation Release 4.2 com o CA EEM Release 8.4 e, em seguida, atualize o CA EEM para a Release 12.x

É possível não realizar uma ação e, ainda assim, usar o CA Process Automation com o CA EEM, contanto que os certificados do CA EEM sejam gerados com os comprimentos de chave padrão. O CA Process Automation pode usar a versão principal 8 do CA EEM SDK para se comunicar com o CA EEM Release 12.x. No entanto, com a versão principal do CA EEM SDK 12, é possível utilizar os novos recursos do CA EEM 12.x.

Recomendamos que você (1) atualize os certificados que o CA Process Automation usa para se comunicar com o CA EEM e (2) atualize o CA Process Automation para usar a versão principal do CA EEM SDK 12. Para fazer isso, execute novamente o instalador. O procedimento a seguir faz referência a números de etapas do tópico Instalar o orquestrador de domínio (na página 96).

- Etapa 5: selecione **Reinstalar** (não Configurar a instalação existente).
- Etapa 16: marque a caixa de seleção **Registrar o aplicativo no CA EEM**.
- Etapa 17: clique em **Registrar**, selecione **Sim** no prompt de atualização e clique em **OK** quando a confirmação de Aplicativo registrado for exibida.

Instale o CA Process Automation Release 4.2 com o CA EEM Release 12.51 e, em seguida, gere novos certificados do CA EEM com os comprimentos de chave 2048 ou 4096

1. O CA Process Automation Release 4.2 é instalado com o CA EEM Release 12.51 usando certificados com comprimentos de chave de 1024 bits.
2. Você pode gerar certificados do CA EEM com comprimentos de chave de 2048 bits (ou 4096 bits).
3. Execute novamente o assistente de instalação do CA Process Automation, mas dessa vez, selecione Configurar instalação existente (e não Reinstalar).
4. Registre o CA Process Automation com o CA EEM. Isto é, registre o valor configurado de "Nome do aplicativo do EEM" com o CA EEM. O processo de registro gera novos certificados do CA Process Automation.

Resultado: os certificados que o CA Process Automation usa ao chamar o CA EEM SDK Release 12.51 coincidem com os comprimentos de chave mais longos usados pelo CA EEM.

Consulte o tópico Exemplo de cenário: configurar a instalação existente para gerar novamente os certificados do CA Process Automation (na página 162).

Configurar o CA EEM para permitir que os usuários referenciados efetuem logon com um nome de email

1. O CA Process Automation Release 4.2 é instalado com o CA EEM usando um armazenamento de usuários referenciado. O armazenamento de usuários referenciado é configurado como vários Active Directories.
2. Durante a instalação do CA Process Automation, você define qual AD deve ser usado como o Active Directory padrão.

   Os usuários referenciados que pertencem ao AD padrão podem efetuar logon no CA Process Automation com nome de usuário não qualificado e senha.
3. Sem a próxima etapa, o CA EEM permite que os usuários referenciados de outros domínios efetuem logon com seus respectivos nomes da entidade principal (*domínio**nome_de_usuário*) e senhas.
4. Configurar o CA EEM para permitir que os usuários referenciados efetuem logon com seus nomes de email (na página 131).

Resultado: os usuários que não estiverem no domínio do AD padrão configurado poderão efetuar logon com seus nomes e senhas principais, onde ambos os seguintes formatos de nome principal são suportados:

nome_de_usuário@*domínio*

*domínio**nome_de_usuário*

Resumo de Registrar o aplicativo no CA EEM

- Se você marcar a caixa de seleção Registrar o aplicativo no CA EEM e essa não for uma nova instalação, clique em **Registrar**. É solicitado que você decida se deseja atualizar o aplicativo do CA Process Automation.
  - Selecione Sim para fazer a atualização para uma nova release.
  - Selecione Sim para gerar certificados do CA Process Automation como parte do processo de configurar a instalação existente.
  - Selecione Não se estiver reinstalando a mesma release e não desejar gerar certificados.

Habilitar as comunicações seguras para o CA Process Automation existente

Se você tiver selecionado HTTP como o protocolo de comunicação do orquestrador de domínio, é possível iniciar a comunicação usando o protocolo HTTPS seguro.

Siga estas etapas:

1. Reinstale o orquestrador de domínio. Especifique a comunicação segura de uma das seguintes maneiras, dependendo do método de instalação:
   - Se reinstalar o orquestrador de domínio de forma interativa (Instalar o orquestrador de domínio (na página 96)), selecione Suporte à comunicação segura.
   - Se criar um arquivo de resposta para a instalação autônoma do orquestrador de domínio, defina a variável isSecure como verdadeiro para ativar as comunicações seguras (HTTPS):
     ```
     isSecure = true
     ```
2. Ative a comunicação segura por agentes de uma das seguintes maneiras, com base em suas configurações.
   - Verifique se os agentes configurados para usar a comunicação obsoleta são reiniciados automaticamente. A comunicação obsoleta é a configuração padrão para os agentes existentes que se comunicam com os orquestradores agrupados que usam um balanceador de carga do Apache. Inicie todos os agentes (na página 182) que foram encerrados antes da reinstalação.
   - Reinstale os agentes que estão configurados para usar a comunicação simplificada. A comunicação simplificada é a configuração padrão para os novos agentes que se comunicam com os orquestradores agrupados que usam um balanceador de carga do NGINX. Reinstale os agentes conforme descrito no tópico Instalando um agente (na página 171). Em seguida, inicie os agentes (na página 182).

   O HTTPS é usado para todas as comunicações entre os agentes e o orquestrador de domínio.
3. Além disso, certifique-se de que todas as instâncias de processo que estejam usando os anexos SOAP existentes tenham sido concluídas.

   Observação: anexos SOAP existentes podem ser acessados apenas por HTTP.
4. Defina regras de firewall para bloquear as comunicações HTTP.

Capítulo 8: Instalar agentes

Esta seção contém os seguintes tópicos:

Pré-requisitos para instalação de agentes

Use as diretrizes a seguir para preparar para a instalação do agente:

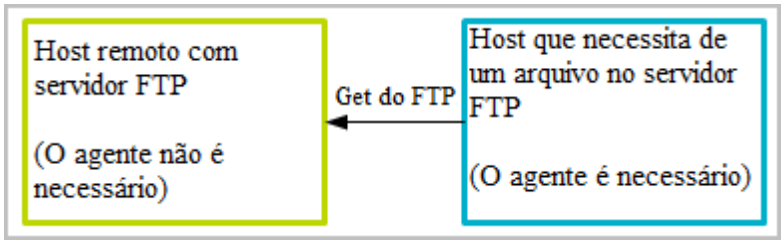
1. Identificar hosts que precisam de agentes (na página 171).
2. Verificar os pré-requisitos do Java para agentes (na página 172).
3. Determinar a disponibilidade de portas para o agente (na página 172) (somente quando uma comunicação obsoleta for utilizada).

Identificar hosts que precisam de agentes

Na maioria dos casos, os operadores são executados em um orquestrador. Isto é, o operador tem como destino um touchpoint para um orquestrador. Os operadores também são executados em hosts com agentes. Nesse caso, o operador tem como destino um touchpoint associado a um ou mais agentes.

Exemplo: instalar agentes em hosts que executam os operadores

Geralmente, você instala agentes do CA Process Automation nos hosts onde os operadores são executados, não em hosts aos quais o operador se conecta durante a execução. Por exemplo, considere um host que precisa de um arquivo no servidor FTP. O host que precisa do arquivo executa o operador Obter FTP. Um agente deve estar instalado no host onde o operador é executado. Nenhum agente é necessário no host com o servidor FTP



Observação: quando não for possível instalar um agente em um host remoto onde um operador deve ser executado, você poderá criar uma conexão SSH entre um host com um agente e o host remoto. Consulte o *Guia de Administrador de Conteúdo* para obter informações sobre touchpoints do proxy.

Verificar os pré-requisitos do Java para agentes

Antes de instalar um agente em um host, verifique se os pré-requisitos do Java são atendidos.

Siga estas etapas:

1. Efetue logon no host. Certifique-se de que a versão com suporte do JRE (Java Runtime Environment) esteja instalada. Se não houver nenhuma versão adequada, faça download do JRE no fornecedor e instale-o.
2. (Opcional) Defina a variável de ambiente JAVA_HOME como o caminho do JRE do agente. Se essa variável não for definida, o instalador do CA Process Automation solicitará que você navegue até o diretório em que o JRE está instalado.

Determinar a disponibilidade de portas para o agente

Esta etapa é necessária somente para os agentes que usam uma comunicação obsoleta. A comunicação simplificada usa portas padrão para HTTP (porta 80) e HTTPS (porta 443).

Os agentes e orquestradores se comunicam uns com os outros pelas seguintes portas.

- Porta do orquestrador: 7001
- Porta do agente: 7003

Durante a instalação do agente, você pode configurar as portas que o agente usa. Ao configurar portas de rede para um agente, aceite as configurações padrão, exceto quando:

- Outro aplicativo no host esteja usando a porta padrão.
- Uma restrição de firewall estiver impedindo a comunicação com a porta padrão.

Para usar uma porta diferente da porta padrão, selecione uma porta não utilizada válida.

Vá até o CA Process Automation e efetue logon.

O URL usado para acessar o CA Process Automation depende se o orquestrador de domínio está configurado com um nó (não agrupado) ou vários nós (agrupado). É possível navegar diretamente para um CA Process Automation não agrupado. Para um CA Process Automation agrupado, procure o balanceador de carga associado. É possível acessar todos os orquestradores no domínio iniciando o URL para o orquestrador de domínio ou para o balanceador de carga para o orquestrador de domínio.

Siga estas etapas:

1. Procure o CA Process Automation.

   - Para uma comunicação segura, use a sintaxe a seguir:
     `https://server:port/itpam`

     Exemplos:
     `https://Orchestrator_host:8443/itpam`
     `https://loadBalancer_host:443/itpam`

   - Para uma comunicação básica, use a sintaxe a seguir:
     `http://server:port/itpam`

     Exemplos:
     `http://Orchestrator_host:8080/itpam`
     `http://loadBalancer_host:80/itpam`

   A página de logon do CA Process Automation é exibida.

2. Digite as credenciais de sua conta de usuário.

   Observação: se o CA EEM estiver configurado para fazer referência a usuários de vários Microsoft Active Directories e o CA Process Automation não aceitar seu nome de usuário não qualificado, digite o nome de sua entidade principal, que é *nome_do_domínio**nome_do_usuário*.

3. Clique em Efetuar logon.

   O CA Process Automation é exibido. A guia Início é exibida.

Mais informações

Sobre a comunicação do agente (na página 158)

Instalar um agente de forma interativa

Os processos podem incluir operadores que precisam ser executados em servidores com um aplicativo, banco de dados ou sistema de destino. Se possível, instale um agente nesse tipo de servidor. Se não for possível, instale o agente em um host que possa se conectar a esse servidor por meio de SSH.

Importante: Antes de instalar um agente, verifique se o Orquestrador de domínio está em execução.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique na paleta Instalação.
3. Clique em Instalar para instalar o agente.

   Uma caixa de diálogo é exibida, mostrando o andamento do download do aplicativo.
4. Se você receber um aviso de segurança, clicar em Executar.

   A caixa de diálogo Seleção de idioma é aberta. O idioma do computador host é selecionado por padrão.
5. Clique em OK ou selecione outro idioma e clique em OK.

   A página de boas-vindas do assistente de instalação do agente do CA Process Automation é exibida.
6. Clique em Avançar.

   O Contrato de Licença é exibido.
7. Leia a licença. Se você aceitar os termos, clique em Eu aceito os termos do Contrato de Licença. Clique em Avançar.

   A página Defina o Java Home Directory é aberta.
8. Se o diretório inicial do Java não for exibido corretamente, procure a pasta JRE.

   Todas as plataformas oferecem suporte à versão jre6; o Windows oferece suporte às versões jre6 e jre7.

   Veja o seguinte exemplo de caminho para a plataforma Windows:

   ```
   C:\Arquivos de programas\Java\jdk1.7.0_45
   ```

9. Clique em Avançar.

   A página Selecionar o diretório de destino é exibida. Em hosts do Windows, o caminho padrão é:

   ```
   C:\Program Files\CA\PAM Agent
   ```

10. Clique em Avançar para aceitar o padrão ou digite um diretório de destino para o novo agente e clique em Avançar.

    A página Selecionar pasta do menu Iniciar é exibida.

11. (Somente no Windows) Clique em Avançar para aceitar o agente do CA Process Automation como o atalho do menu Iniciar ou digite um novo nome e clique em Avançar.

    - (Opcional) Crie atalhos para todos os usuários nesse host.
    - (Opcional) Não criar uma pasta no menu Iniciar.

12. Examine o URL do domínio. Este é o URL a partir do qual você iniciou a instalação do agente. Clique em Avançar.

13. Se o domínio estiver protegido, forneça uma senha.

14. Preencha a página Propriedades gerais e, em seguida, clique em Avançar.

    a. Digite o nome do host do agente para Host do agente. Esse nome identifica o host a partir do qual você iniciou a instalação.

    b. Altere ou aceite o Nome de exibição padrão, o nome do host.

    c. Se você tiver iniciado a instalação do agente em um host do Windows, selecione Instalar como um serviço do Windows.

    d. Para forçar uma nova conexão para cada comunicação de um orquestrador a um agente, selecione Usar comunicação obsoleta.

       Recomendamos deixar essa caixa de seleção *desmarcada*. A comunicação simplificada, o padrão, é preferencial porque usa uma conexão persistente.

    e. Se você tiver selecionado Usar comunicação obsoleta, aceite 7003 como a Porta do agente, a menos que essa porta esteja em uso. Se a porta padrão estiver em uso, digite um número de porta sem uso, como 57003, como a porta na qual o agente escuta a comunicação com os orquestradores.

       Observação: se a comunicação obsoleta não for usada, os orquestradores usarão uma conexão de soquete da web (estabelecida por agentes) para se comunicar com os agentes. Os orquestradores usam a porta 80 para se comunicar com agentes por HTTP. Os orquestradores usam a porta 443 para se comunicar com agentes por HTTPS.

    f. Selecione Iniciar agente após a instalação.

       A inicialização do agente permite exibir o agente ativo e continuar com a configuração do agente.

15. Clique em Avançar para aceitar o diretório temporário padrão para executar os scripts ou digite outro caminho e, em seguida, clique em Avançar.

    Observação: um caminho aceitável não contém espaços.

    A página Definir a diretiva de execução do PowerShell é exibida.

16. Preencha a configuração de uma das seguintes maneiras.

    - Para executar os scripts do Windows PowerShell por meio desse agente:
      a. Marque a caixa de seleção Definir a diretiva de execução do PowerShell.
      b. Vá até o local do host do PowerShell, se for diferente do padrão exibido.
      c. Clique em Avançar.
    - Se você não usar o Windows PowerShell, clique em Avançar.

    A instalação do agente é iniciada.

17. Clique em Concluir.

18. (Somente no Windows) Inicie o serviço do agente. Clique em Iniciar, Programas, CA, Agente do CA Process Automation, Iniciar serviço do agente.

19. Clique na paleta Navegador de configuração, na guia Configuração.

20. Clique em Atualizar. (Ou, efetue logoff e logon novamente.)

21. Expanda Agentes e verifique se o nome do seu agente está listado.

    Observação: para usar o host do agente como um destino, configure um touchpoint. Para usar o agente do host como um gateway para um host remoto, configure um touchpoint do proxy.

Executar uma instalação autônoma do agente

O CA Process Automation oferece suporte à instalação autônoma do agente para permitir que os administradores instalem os agentes remotamente em um computador host. Você pode usar uma instalação autônoma para incluir o agente na rotina de configuração inicial para configurar novos computadores host. Você também pode usar a instalação autônoma para oferecer suporte à instalação através das soluções de fornecimento do software.

Quando você digita o URL de domínio com o -VdomainUrl=*domain_url*, o *domain_url* é http(s):<*FQDN_of_Domain_Orchestrator*>:<*port_number*>.

Importante: O *domain_url* deve ser inserido sem **/itpam/**.

Você pode executar uma instalação autônoma do agente.

Siga estas etapas:

1. Efetue logon como administrador no servidor onde o orquestrador de domínio estiver instalado.
2. Verifique se o orquestrador de domínio está sendo executado.

   Observação: um instalador de agente autônomo ainda deve ter conectividade com o orquestrador de domínio para instalar um agente com êxito.
3. Vá até o seguinte diretório:

   `install_dir/server/c2o/.c2orepository/media`

   A pasta de mídia inclui os seguintes arquivos:

   - AgentInstaller
   - AgentInstaller.sh
   - AgentInstaller_64
   - AgentInstaller-hpux.sh
   - CA_PAM_Agent_unix.sh
   - CA_PAM_Agent_windows_32
   - CA_PAM_Agent_windows_64
4. Localize dois arquivos para o seu sistema operacional:
   - Windows de 32 bits: AgentInstaller.bat e CA_PAM_Agent_windows_32.exe
   - Windows de 64 bits: AgentInstaller_64.bat e CA_PAM_Agent_windows_64.exe
   - Linux UNX: Agente Install.sh e CA_PAM_Agent_unix.sh
   - HP-UX: AgentInstaller-hpux.sh e CA_PAM_Agent_unix.sh
5. Copie os arquivos para o seu sistema operacional em um diretório no host em que deseja instalar o agente.
6. Efetue logon no host em que deseja instalar o agente e navegue até o diretório em que você copiou o instalador do agente e os arquivos wrapper.
7. (Opcional) Execute o instalador do agente sem argumentos para exibir a ajuda.
8. Use os seguintes argumentos da linha de comando com o instalador do agente:

   ```
   AgentInstaller.bat -VdomainUrl=domain_url -VacceptLicense=true
   [-option1 -option2 ...]
   AgentInstaller.sh -VdomainUrl=domain_url
   –VacceptLicense=true[-option1 -option2 ...]
   ```

   Por exemplo:

   `-VdomainURL=https://domainserver.company.com:8443-VacceptLicense=true`

```
-VdomainURL=http://domainserver.company.com:8080
```

O instalador do agente aceita as seguintes opções da linha de comando:

–VlisteningAddress=*hostname*

Especifica o nome de domínio totalmente qualificado ou o endereço IP da máquina host na qual você está instalando o agente. Isso será necessário se a máquina host tiver várias interfaces de rede.

-VdisplayName=*display_name*

Especifica o nome que é exibido para esse agente.

-VnodePort=*port_number*

Especificar a porta a ser usada no host.

-VwinService=*boolean*

Defina o valor como true para instalar o agente como um serviço do Windows.

-Vsys.installationDir=*path*

Especificar o caminho completo para a instalação no host.

-VstartAgent=*boolean*

Defina o valor como true para iniciar o agente quando a instalação for concluída.

-VjavaHome=*value*

Especificar o Local inicial do Java.

-Vscripts.tmpDir=*value*

Especifica o diretório temporário para executar os scripts.

VcertPassword=*value*

Especifica a senha do certificado como configurado no orquestrador de domínio. Esse valor é obrigatório quando você estiver usando SSL e/ou estiver trabalhando no modo Seguro.

VisLookUpDNSForIP=*boolean*

Defina o valor como true para procurar o nome do host do agente a partir do DNS.

jetty.ssl.ciphers=*value*

A lista de cifras separadas por vírgulas que deve ser usada durante a comunicação do agente com o orquestrador de domínio.

-VsetPowerShellExecPolicy=*value*

A execução de scripts do PowerShell na plataforma Windows requer a configuração da diretiva de execução como "Remote Signed". Para executar os scripts do PowerShell por meio do CA Process Automation, defina o valor dessa variável como true.

-VpowerShellPath=*value*

Especifica o caminho do PowerShell na máquina host.

-VdeprecatedComms=*boolean*

Especifica o modo de comunicação (na página 158). Defina o valor como true para oferecer suporte ao modo de comunicação obsoleta. Defina o valor como false para oferecer suporte ao novo modo de comunicação.

Tarefas de pós-instalação para agentes

As tarefas de pós-instalação para agentes são condicionais.

- Se houver um conflito de porta depois da instalação de um agente, você poderá resolver o conflito de porta com o agente (na página 180).
- Se sua empresa não permitir a execução de agentes com privilégios de raiz, você poderá executar programas para configurar agentes para executar como o usuário padrão com poucos privilégios (na página 181).
- Os agentes instalados com o CA Process Automation Release 4.2 usam a comunicação simplificada por padrão. Consulte o *Guia do Administrador de Conteúdo* para saber como configurar os agentes para utilizar a comunicação obsoleta, se estiver usando um balanceador de carga do Apache. Se você acabou de atualizar para o CA Process Automation Release 4.2, consulte o tópico sobre como configurar os agentes existentes para usar a comunicação simplificada.

Resolver o conflito de porta com o agente

Se uma porta ficar indisponível após a instalação de um agente, altere a atribuição de porta usando uma das seguintes abordagens:

- **Windows**:
  1. Navegue até o seguinte diretório no host no qual o agente está instalado:
     `diretório_instalação_agente\.config`
  2. Abra o seguinte arquivo em um editor:
     `OasisConfig.properties`
  3. Modifique a seguinte atribuição de porta:
     `oasis.jxta.port=`
  4. Salve o arquivo. Feche o arquivo.
  5. Vá até o seguinte diretório no servidor no qual o orquestrador de domínio está instalado:
     `install_dir/server/c2o/.system`
  6. Remover a pasta .c2o, se ela existir.
- **UNIX ou Linux**: ajuste a configuração de inicialização.

Configurar agentes para serem executados como usuário padrão com poucos privilégios

Os programas descritos nesta seção se aplicam a um agente instalado em um host com um sistema operacional Windows. Esses programas fazem o seguinte:

- Criam a conta de usuário padrão usada para todos os agentes do CA Process Automation.
- Atribuem a esse agente os direitos necessários no host local.

Observação: esses programas não foram validados para funcionar com todas as versões do Windows.

Se esses programas não funcionarem na sua versão do Windows, defina as configurações manualmente. Use o Editor de Política de Grupo nas Ferramentas Administrativas do Windows.

Antes de começar, determine o *nome_do_usuário* ou *nome_do_grupo* da conta de usuário a ser utilizado como padrão em todos os agentes e orquestradores instalados. Você pode usar uma conta de usuário comum. Não é necessário que seja uma conta de domínio com direitos administrativos.

Siga estas etapas:

1. Abra um prompt de comando. Por exemplo, Executar cmd.
2. Navegue até o seguinte diretório:

   diretório_instalação_agente\PAMAgent\.c2orepository\public\tools
3. Digite o seguinte comando:

   `itpamsvcacct.bat user_name|group_name`

   A conta de usuário é criada com o nome que você especificou.
4. Digite os cinco comandos a seguir. (Você pode digitar um único comando e usar um espaço como delimitador entre os direitos.)

   `itpamassgnrights.exe user_name host_name + SeTcbPrivilege`

   `itpamassgnrights.exe user_name host_name + SeCreateTokenPrivilege`

   `itpamassgnrights.exe user_name host_name + SeServiceLogonRight`

   `itpamassgnrights.exe user_name host_name + SeBatchLogonRight`

   `itpamassgnrights.exe user_name host_name + SeAssignPrimaryTokenPrivilege`

   A conta de usuário especificada possui os privilégios necessários para executar o agente no host local especificado.

Como iniciar ou interromper um agente

A maneira de iniciar e interromper um agente depende do sistema operacional usado pelo host em que o agente está instalado.

- Iniciar um agente (na página 182).
- Interromper um agente. (na página 183)

Iniciar um agente

Use o método de início ou reinício do agente para o sistema operacional no host que contém o agente.

Iniciar ou reiniciar um agente em um host do Microsoft Windows

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional Windows.

Siga estas etapas:

1. Efetue logon no host do Windows em que um agente esteja instalado.
2. No menu Iniciar, selecione Programas, CA, Agente do CA Process Automation, Iniciar serviço do agente.
3. Efetue logoff do servidor.

Iniciar ou reiniciar um agente em um host do Linux

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional UNIX ou Linux.

Siga estas etapas:

1. Efetue logon no host do UNIX ou Linux em que um agente esteja instalado.
2. Altere os diretórios para:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```
3. Execute o seguinte comando:

   ```
   ./c2oagtd.sh start
   ```

   O agente é reiniciado.

Interromper um agente

É possível interromper um agente do CA Process Automation que está sendo executado em um host do UNIX ou Linux.

Interromper um agente em um host do Microsoft Windows

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional Windows.

Siga estas etapas:

1. Efetue logon no host do Windows em que um agente esteja instalado.
2. No menu Iniciar, selecione Programas, CA, Agente do CA Process Automation, Interromper serviço do agente.
3. Efetue logoff do servidor.

Interromper um agente em um host Linux

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional UNIX ou Linux.

Siga estas etapas:

1. Efetue logon no host do UNIX ou Linux em que um agente esteja instalado.
2. Altere os diretórios para:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Execute o seguinte comando:

   ```
   ./c2oagtd.sh stop
   ```

   A execução do agente é interrompida.

Capítulo 9: Adicionar um nó ao orquestrador de domínio

É possível criar o domínio do CA Process Automation estendendo a capacidade do orquestrador de domínio. A adição de um nó de agrupamento ajuda a atingir alta disponibilidade para o orquestrador de domínio. Use o mesmo processo para atualizar um nó que foi usado para adicionar um nó.

Esta seção contém os seguintes tópicos:

Pré-requisitos para instalação de um nó de agrupamento para o orquestrador de domínio

Você pode instalar um nó de agrupamento para o orquestrador de domínio Um nó de agrupamento estende a potência de processamento do orquestrador de domínio e, portanto, pode melhorar o desempenho. Um nó de agrupamento compartilha os mesmos bancos de dados que foram configurados para os outros nós existentes, que fazem parte de um agrupamento do orquestrador de domínio.

Antes de instalar o produto, execute os seguintes pré-requisitos:

Siga estas etapas:

1. Identifique um host para o nó de agrupamento do orquestrador que atenda aos requisitos de plataforma e hardware. Consulte o componente do orquestrador nos dois seguintes tópicos:
   - Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30).
   - Requisitos de hardware (na página 32).
2. Verifique se o host para esse nó de agrupamento está na mesma sub-rede que outros nós existentes, que fazem parte do orquestrador de domínio.
3. Verifique se o host para esse nó de agrupamento está no mesmo fuso horário que outros nós existentes, que fazem parte do orquestrador de domínio.
4. Verifique se o host para esse nó de agrupamento tem um JDK suportado e, se estiver ausente, baixe-o.

   Consulte o tópico Pré-requisitos do JDK (na página 76).
5. Se o host para esse nó de agrupamento estiver executando uma versão recente de um sistema operacional Windows, consulte a opção Controle de Conta de Usuário (no Painel de Controle, Contas de Usuário). Se essa opção estiver ativada, desmarque a caixa de seleção e reinicialize o servidor.

6. Se o orquestrador de domínio tiver sido configurado com um balanceador de carga F5, adicione esse nó ao balanceador de carga.

   Consulte Criar um nó do F5 para cada nó de agrupamento (na página 54).

7. Se o orquestrador de domínio tiver sido configurado com um balanceador de carga do Apache, adicione esse nó ao balanceador de carga.

   a. Vá até *apache_install_location*\conf.

   b. Abra o arquivo workers.properties.

   c. Remova o comentário das seguintes linhas em Definir nó 2 no arquivo worker.properties.

      ```
      worker.node2.port=8009
      worker.node2.host=hostname
      worker.node2.type=ajp13
      worker.node2.lbfactor=1
      ```

   d. Altere *hostname* para o nome do host do servidor onde o nó do orquestrador de domínio está sendo instalado.

   e. Adicione "node2" à linha worker.loadbalancer.balance_workers= no comportamento de balanceamento de carga. A entrada se parece com as seguintes informações:

      ```
      worker.loadbalancer.balance_workers=node1,node2
      ```

      Observação: para o terceiro nó e os nós subsequentes, siga as mesmas instruções, mas substitua node2 pelo número do nó correto, por exemplo, node3 ou node4.

   f. Reinicie o Apache.

8. Se o primeiro nó do orquestrador de domínio tiver sido configurado com um balanceador de carga NGINX, adicione esse nó (node2) ao balanceador de carga.

   a. Vá até o arquivo pam-server.conf e abra-o.

   b. Localize a linha #Define node2. (Os dados do node1 fazem referência ao primeiro nó do orquestrador de domínio; ignore as seções que se referem ao node1.)

      Observação: o *node2_hostname* é o endereço IP ou o nome DNS do host onde o node2 está instalado. O valor *jetty_server_port* é da opção Porta do servidor, fornecido durante a instalação do primeiro nó do orquestrador de domínio. Digite 80 para a comunicação simplificada ou digite 7003 para a comunicação obsoleta.

   c. Crie as seguintes entradas no pam-server.conf para definir o node1 e o novo nó, node2:

      ```
      // node1 is the worker node name
      upstream node1{
        # Define node1
      ```

```
  server node2_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
// node2 is the worker node name
upstream node2{
  # Define node2
  server node2_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
```

d. Dentro da tag de servidor, crie as seguintes entradas para o node1 e o novo nó, node2:

```
Server{

...
    location = /ws {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/ {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/node1 {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location /ws/node1/ {
               // node1 is the upstream name provided above
               proxy_pass http://node1;
               }
    location = /ws/node2 {
               // node2 is the upstream name provided above
                proxy_pass http://node2;
               }
    location /ws/node2/ {
               // node2 is the upstream name provided above
               proxy_pass http://node2;
               }
}
```

Instalar um nó agrupado para o orquestrador de domínio

Os usuários com privilégios PAMAdmin podem opcionalmente adicionar nós de agrupamento para um orquestrador de domínio. O agrupamento ajuda a balancear a carga de processamento em todos os hosts agrupados. O agrupamento é um bom modo de promover alta disponibilidade. Para que o orquestrador de domínio seja elegível para agrupamento, você deve ter instalado um balanceador de carga antes de instalar o orquestrador de domínio.

Verifique se os Pré-requisitos para instalação de um nó de agrupamento para o orquestrador de domínio (na página 186) foram atendidos. Em seguida, instale o nó de agrupamento.

Siga estas etapas:

1. Efetue logon no servidor em que você planeja instalar esse nó de agrupamento para o orquestrador de domínio.
2. Vá até o URL do orquestrador de domínio e efetue logon.

   `https://nome_do_host_do_balanceador_de_carga:8443/itpam`

   `http://nome_do_host_do_balanceador_de_carga:8080/itpam`
3. Clique na guia Configuração.
4. Clique na paleta Instalação.
5. Clique em Instalar para instalar o nó de agrupamento para o orquestrador de domínio.
6. Se a assinatura digital não puder ser verificada, clique em Executar para iniciar a instalação.
7. Em Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation, clique em Avançar.
8. Aceite o contrato de licença e clique em Avançar.
9. Especificar o diretório de destino para instalar o nó do orquestrador e clicar em Avançar.

   O instalador criará a pasta automaticamente se ela não existir.
10. Na tela Pré-requisitos para instalação do CA Process Automation, clique em Avançar.

    A opção Concluindo o assistente de instalação do CA Process Automation para pré-requisitos exibe uma caixa de seleção Usar domínio e um caminho. Verifique se essa caixa de seleção está marcada. O processo de instalação usa as informações reunidas na instalação do orquestrador de domínio. Essa caixa de seleção normalmente não é alterada durante a instalação, mas se for necessário inserir novas informações, clique na caixa de seleção e digite essas informações.
11. Clique em Concluir para iniciar a instalação do nó de agrupamento para o orquestrador de domínio.

12. Na tela de boas vindas, clique em Avançar.
13. Aceite o contrato de licença e clique em Avançar.
14. Aceite o caminho exibido ou vá até o diretório inicial do Java. Clique em Avançar.

    O JDK é validado e a instalação do orquestrador é iniciada. Levará um minuto para copiar os arquivos de configuração.
15. Preencha a Tela de configuração e clique em Avançar.

    orquestrador

    Especifica o orquestrador ao qual o nó de agrupamento será adicionado. O orquestrador selecionado na lista suspensa deve ser configurado com um nome do host público que especifica o FQDN do servidor no qual o balanceador de carga está instalado.

    Nó de trabalho do balanceador de carga

    Especifica o nome do nó, por exemplo, node 2. Esse é o nome do nó especificado no arquivo workers.properties do Apache, em que *hostname* é o nome do host no qual você está instalando o nó de agrupamento:

    worker.**node2**.host=*hostname*.*mycompany*.com

    Observação: a primeira instalação do orquestrador de domínio é o node1. Para o segundo nó, digite **node2**.
16. Exiba o Nome da empresa e clique em Avançar.
17. Digite a senha do certificado e clique em Avançar.

    Senha do certificado

    Especifica a *mesma* senha do certificado que foi inserida durante a instalação dos nós anteriormente instalados do orquestrador de domínio.
18. Verifique as entradas nas propriedades gerais para o orquestrador. A maioria das configurações é derivada da instalação do orquestrador de domínio. Clique em Avançar.

    Host do servidor

    Especifica o FQDN do host no qual esse nó de agrupamento para o orquestrador de domínio está sendo instalado.
19. Selecione a pasta do menu iniciar e clique em Avançar.
20. Exiba as configurações do PowerShell.
21. Exiba as configurações de segurança do CA EEM e clique em Avançar.
22. Exiba as configurações do banco de dados para o banco de dados do repositório (biblioteca) e clique em Avançar.
23. Exiba as configurações do banco de dados para o banco de dados de tempo de execução e clique em Avançar.

24. Exiba as configurações do banco de dados para o banco de dados de relatórios e clique em Avançar.
25. Monitore as mensagens de andamento enquanto o instalador instala o nó de agrupamento para o orquestrador de domínio no mesmo computador no qual você iniciou a instalação.
26. Clique em Concluir.

    O nó de agrupamento para o orquestrador de domínio está instalado.

Sincronizar a hora para um nó de agrupamento

Todos os nós de agrupamento para qualquer orquestrador devem ter exatamente a mesma hora do relógio, sincronizada com um servidor de tempo externo padrão. Considere uma das seguintes abordagens para sincronizar a hora de todos os nós em um agrupamento:

- Sincronize todos os orquestradores e nós de agrupamento com um servidor de tempo externo padrão (preferencial).
- Sincronize manualmente a hora de todos os nós de agrupamento adicionais, da seguinte maneira:
  1. Verifique a exatidão da hora de todos os nós de agrupamento.
  2. Execute o comando do sistema operacional apropriado em cada nó de agrupamento para sincronizar a hora de todos eles.

Capítulo 10: Instalar um orquestrador adicional

Depois de instalar o orquestrador de domínio, você pode criar o domínio instalando orquestradores adicionais. Você pode instalar vários orquestradores em um ambiente. Se você criar um novo ambiente, por exemplo, para uso de produção, instale um orquestrador nesse ambiente.

Esta seção contém os seguintes tópicos:

Pré-requisitos para instalação de um orquestrador

É possível instalar um orquestrador no ambiente com o orquestrador de domínio ou em um ambiente separado. Antes de instalar um orquestrador, execute os seguintes pré-requisitos:

Siga estas etapas:

1. Identifique um host para o orquestrador que atenda aos requisitos de plataforma e hardware. Consulte o componente do orquestrador nos dois seguintes tópicos:
   - Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30).
   - Requisitos de hardware (na página 32).
2. Verifique se o host para o orquestrador tem um JDK suportado e, se estiver ausente, baixe-o.

   Consulte o tópico Pré-requisitos do JDK (na página 76).

3. Tenha à mão a senha do certificado que corresponde à senha do armazenamento de chaves no orquestrador de domínio. Essa senha controla o acesso para as chaves usadas para criptografar senhas e outros dados críticos.

   Importante: Não é possível instalar com êxito outro orquestrador sem essa senha.

4. Identifique o servidor ou os servidores de banco de dados para hospedar o banco de dados de tempo de execução e, opcionalmente, o banco de dados do repositório (biblioteca) deste orquestrador. Analise os seguintes fatores:

   - Cada orquestrador deve ter seu próprio banco de dados de tempo de execução.
   - Um orquestrador pode compartilhar o banco de dados da biblioteca do orquestrador de domínio ou possuir seu próprio banco de dados.
   - Geralmente, todos os orquestradores no domínio usam o banco de dados de relatórios criado para o orquestrador de domínio.
   - Um servidor de banco de dados deve atender aos requisitos de plataforma e hardware. Consulte o componente do servidor de banco de dados nos dois seguintes tópicos:
     - Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30).
     - Requisitos de hardware (na página 32).

5. Prepare o servidor de banco de dados. Os bancos de dados do repositório e de tempo de execução podem ser criados em diferentes servidores de banco de dados.

   Consulte o tópico Pré-requisitos do servidor de banco de dados (na página 69).

6. Avalie a necessidade de um balanceador de carga para esse orquestrador. O CA Process Automation oferece suporte aos seguintes métodos de balanceamento de orquestradores agrupados.

   Observação: é recomendável um balanceador de carga de hardware. Consulte o tópico Pré-requisitos do balanceador de carga F5 (na página 53). Se isso não for possível, recomendamos o NGINX como o balanceador de carga de software de sua escolha. O NGINX para UNIX é altamente escalonável. O NGINX para Windows pode oferecer suporte a até 300 agentes usando a comunicação simplificada. Consulte o tópico Pré-requisitos do balanceador de carga NGINX.

7. Se planejar agrupar esse orquestrador usando NGINX, execute as seguintes etapas adicionais:

   a. Vá até o arquivo pam-server.conf e abra-o.

   b. Localize a linha #Define node1. (Os dados do node1 fazem referência ao nó do orquestrador que foi instalado primeiro.)

   c. Digite os dados a seguir, em que *jetty_server_port* é o valor configurado para Porta do servidor durante a instalação. Em geral, os valores são 80 para a comunicação simplificada ou 7003 se os agentes que se conectam a esse orquestrador usarem a comunicação obsoleta.

```
// node1 is the worker node name
upstream node1{
  # Define node1
  server node1_hostname:jetty_server_port max_fails=3
fail_timeout=3s;
}
```

   d. Dentro da tag de servidor, crie as seguintes entradas:

```
Server{
       location = /ws {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location = /ws/ {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location = /ws/node1 {
                 // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
       location /ws/node1/ {
                // node1 is the upstream name provided above
                proxy_pass http://node1;
                }
```

```
...
                    }
}
```

8. Identifique um servidor de tempo (servidor NTP). Configurar todos os orquestradores para usar o mesmo servidor de tempo externo (ou servidor de tempo local) é a melhor maneira de garantir a sincronização.
9. Verifique se os seguintes componentes foram iniciados antes de ir para o CA Process Automation e iniciar a instalação de um orquestrador:
   - CA EEM.
   - O balanceador de carga, se usado.
   - O serviço do orquestrador de domínio.
   - O servidor de banco de dados que você deseja usar para o banco de dados de tempo de execução e, opcionalmente, um banco de dados do repositório (biblioteca) separado.

Instalar um orquestrador

Depois de instalar o orquestrador de domínio, você pode adicionar orquestradores em outros hosts. Cada novo ambiente precisa de ao menos um orquestrador, mas pode haver mais de um. Vários orquestradores permitem a segmentação. Novos orquestradores herdam as informações do CA EEM do orquestrador de domínio.

Antes de usar o procedimento a seguir, atenda aos pré-requisitos para instalar um orquestrador (na página 193). Por exemplo, verifique se você tem um JDK instalado.

Use o processo a seguir para instalar um orquestrador ou para fazer a atualização de um orquestrador existente.

Siga estas etapas:

1. Efetue logon no servidor em que deseja instalar o novo orquestrador.
2. Navegue até o CA Process Automation e efetue logon (na página 173) com as credenciais de administrador. Por exemplo, efetue logon como um membro do grupo PAMAdmins.
3. Clique na guia Configuração e selecione a paleta Instalação.
4. Clique no link de pré-requisitos e verifique se todos os pré-requisitos foram atendidos.

5. Clique em Instalar orquestrador.

   Se você usar o navegador da web Firefox, abra-o com o iniciador do Java Web Start (o padrão).

   Se necessário, instale o certificado conforme instruído. O aplicativo é baixado. A caixa de diálogo Seleção de idioma pode aparecer na bandeja do sistema.

6. Selecione um idioma e clique em OK.

   A página Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation é exibida.

7. Clique em Avançar.

8. Aceitar o Contrato de licença e clicar em Avançar.

9. Aceite o diretório de instalação padrão (install_dir) ou altere-o e clique em Avançar.

10. Clique em Avançar na página Pré-requisitos para instalação do CA Process Automation.

    A página Instalando o JBoss mostra o andamento da instalação do jboss-5.1.

11. Especifique o jars do JDBC para instalação de uma das seguintes maneiras:

    - Deixe a caixa de seleção Usar domínio selecionada e clique em Avançar. Isso especifica o uso dos JDBC Jars que a instalação do orquestrador de domínio configurou.
    - Conclua o seguinte procedimento:

      a. Desmarque a caixa de seleção Usar domínio.

      b. Clique em Adicionar arquivos.

      c. Selecione o tipo de servidor de banco de dados.

      d. Clique em Procurar e navegue até o arquivo JDBC JAR do tipo de servidor selecionado.

      e. Clique em Avançar.

12. Na tela de confirmação, clique em Avançar.

13. Clique em Concluir para avançar para o instalador do CA Process Automation.

14. Clique em Avançar na página de boas-vindas.

15. Aceite o contrato de licença e clique em Avançar.

16. Execute uma das seguintes ações na página do Diretório inicial Java:

    - Clique em Avançar para aceitar o padrão.
    - Navegue até o local do JDK e clique em Avançar.

17. Exiba o URL do domínio e clique em Avançar.

18. Se você não estiver usando o Single Sign-on (logon único) em um balanceador de carga, clique em Avançar e ignore a etapa a seguir.
19. Preencha essa página e clique em Avançar.

Configurar o SSO (Single Sign-On - Logon único)

Especifica se você está usando o CA SiteMinder com o SSO, em que o padrão é desmarcado. Selecionar essa opção ativa esses campos:

- Tipo de autenticação de SSO (Cabeçalho)
- Parâmetro de autenticação de SSO (sm-user)
- Tipo de servidor (Novo orquestrador)

Configurar o balanceador de carga

Especifica se é preciso instalar esse orquestrador para que possa agrupar.

Selecionado

Indica se um balanceador de carga está configurado para este orquestrador.

Desmarcado

Indica que nenhum balanceador de carga está configurado para este orquestrador.

Nó de funcionário do balanceador de carga (Apache)

Especifica o nome desse nó. Como este orquestrador é o primeiro nó deste agrupamento, especifique **node1**.

Observação: para nós diferentes do node1 (por exemplo, node2), consulte:

- Adicionando um nó ao orquestrador de domínio (na página 185).
- Adicionando um nó a um orquestrador adicional (na página 203).

Nome do host público

Especifica o nome do host público, como no exemplo a seguir:

loadbalancerhost.*mycompany*.com

- Se o orquestrador de domínio usa o Single Sign-On (SSO), esse campo especificará o FQDN do aplicativo IIS (Serviços de Informações da Internet) ou o aplicativo Apache com o CA SiteMinder WebAgent.
- Se o orquestrador de domínio não usar o Single Sign-On (SSO), esse campo especificará o FQDN do balanceador de carga.

Número da porta do host público

Se Suporte à comunicação segura estiver desmarcada, esse campo especificará a porta HTTP para o host público (IIS ou Apache).

Padrão

80

Porta segura do host público

Se Suporte a comunicação segura estiver selecionado, esse campo especifica a porta HTTPS para o host público (IIS ou Apache).

Padrão

443

Suporte a comunicação segura

Especifica se o host público usa HTTPS para comunicação segura.

Selecionado

O host público usa HTTPS para comunicação segura.

Desmarcado

O host público não usa HTTPS para comunicação segura. Em vez disso, ele usa HTTP para comunicação básica.

20. Exiba o Nome da empresa e clique em Avançar.
21. Digite a senha do certificado que o orquestrador de domínio usa e clique em Avançar.

    Se essa senha do certificado tiver sido perdida ou esquecida, você deverá reinstalar todos os orquestradores no sistema do CA Process Automation, começando com o orquestrador de domínio.
22. Especifique as preferências para a pasta do menu Iniciar e clique em Avançar.
23. Digite as propriedades gerais para o orquestrador de domínio e clique em Avançar.

    Host do servidor

    Especifica o FQDN deste orquestrador.

    Nome de exibição

    Especifica o nome que o navegador de configuração exibe para esse orquestrador.

    - Se você não configurar um balanceador de carga, o nome de exibição será o nome do host do servidor.
    - Se você configurar um balanceador de carga, o nome de exibição será o FQDN do servidor que hospeda o balanceador de carga.
24. Aceite o padrão ou defina o diretório temporário no qual executar scripts e, em seguida, clique em Avançar.
25. Defina a diretiva de execução do PowerShell e clique em Avançar.

26. Digite as configurações do Banco de dados do repositório para esse orquestrador de uma das seguintes maneiras:
    - Para compartilhar o banco de dados Repositório (Biblioteca) que o orquestrador de domínio usa, conclua o seguinte procedimento:
        a. Insira as mesmas informações que você configurou para o orquestrador de domínio.
        b. Clique em Testar configurações do banco de dados.
        c. Clique em Avançar.
    - Para criar um banco de dados Repositório (Biblioteca) separado para esse orquestrador, conclua o seguinte procedimento:
        a. Preencha todos os campos.
        b. Forneça um nome exclusivo para o banco de dados do repositório.
        c. Clique em Criar banco de dados.
        d. Clique em Testar configurações do banco de dados.
        e. Clique em Avançar.
27. Insira as configurações do banco de dados de tempo de execução. Cada orquestrador exige um banco de dados de tempo de execução separado.
    a. Se o novo banco de dados Tempo de Execução residir no mesmo servidor do banco de dados Repositório desse orquestrador, clique em Copiar do repositório principal para copiar o nome de usuário e a senha definidos.
    b. Se o servidor de banco de dados especificado hospedar outros bancos de dados de tempo de execução, crie um nome exclusivo válido para esse banco de dados de tempo de execução.
    c. Clique em Criar banco de dados.
    d. Clique em Testar configurações do banco de dados.
    e. Clique em Avançar.
28. Exiba as Configurações do banco de dados de relatórios e clique em Avançar. Todos os orquestradores no domínio compartilham o mesmo banco de dados de Relatórios.
29. Clique em Concluir.

Tarefas pós-instalação para um orquestrador

Execute as tarefas pós-instalação a seguir, conforme necessário.

1. Para configurar um balanceador de carga do Apache para uma comunicação segura via SSL, execute as seguintes etapas:
   a. Navegue até a seguinte pasta:
   apache_install_dir\conf\extra\
   b. Abra o seguinte arquivo:
   `httpd-ssl.conf`
   c. Adicione as seguintes linhas dentro das tags <VirtualHost> </VirtualHost> ao final do arquivo:

   ```
   SSLOptions +StdEnvVars +ExportCertData
   JkMount /* loadbalancer
   ```

   Observação: para configurar um balanceador de carga para usar comunicações básicas, comente a instrução anterior.
   d. Salve o arquivo. Feche o arquivo.
   e. Reinicie o servidor HTTP Apache.
2. Configure as portas (na página 92).
3. Configure os firewalls para comunicação bidirecional (na página 128).
4. Se tiver instalado o orquestrador de domínio em um servidor com o sistema operacional HP-UX, execute as etapas de configuração adicionais no HP-UX.
5. (Somente no Windows) Inicie o serviço do orquestrador.

   O orquestrador registra a si mesmo como orquestrador de domínio.
6. Verifique a instalação do orquestrador adicional.
   a. Navegue até o CA Process Automation e efetue logon.
   b. Clique na guia Configuração.
   c. Clique no nó Orquestradores na paleta Navegador de configuração.
   d. Visualize o novo orquestrador nessa lista.

Capítulo 11: Adicionar um nó a um orquestrador adicional

Após a instalação de um orquestrador adicional, você pode ampliar sua capacidade e fornecer o recurso de tolerância a falhas adicionando um nó de agrupamento. Se um nó falhar, outro nó assumirá o controle. Você pode usar a instalação interativa ou a instalação autônoma para instalar os nós de agrupamento.

Esta seção contém os seguintes tópicos:

Pré-requisitos para instalação de um nó de agrupamento para um orquestrador

Você pode instalar um nó de agrupamento para um orquestrador. Um nó de agrupamento estende a potência de processamento de um orquestrador e, portanto, pode melhorar o desempenho. Um nó de agrupamento compartilha os mesmos bancos de dados que foram configurados para os outros nós existentes, que fazem parte do agrupamento do orquestrador.

Antes da instalação, execute os seguintes pré-requisitos:

Siga estas etapas:

1. Identifique um host para o nó de agrupamento do orquestrador que atenda aos requisitos de plataforma e hardware. Consulte o componente do orquestrador nos dois seguintes tópicos:
   - Suporte à plataforma e requisitos para componentes do CA Process Automation (na página 30).
   - Requisitos de hardware (na página 32).
2. Verifique se o host para esse nó de agrupamento está na mesma sub-rede que outros nós existentes, que fazem parte do orquestrador.
3. Verifique se o host para esse nó de agrupamento está no mesmo fuso horário que outros nós existentes, que fazem parte do orquestrador.
4. Verifique se o host para esse nó de agrupamento tem um JDK suportado e, se estiver ausente, baixe-o.

   Consulte o tópico Pré-requisitos do JDK (na página 76).
5. Se o host para esse nó de agrupamento estiver executando uma versão recente de um sistema operacional Windows, consulte a opção Controle de Conta de Usuário (no Painel de Controle, Contas de Usuário). Se essa opção estiver ativada, desmarque a caixa de seleção e reinicialize o servidor.

6. Se o orquestrador tiver sido configurado com um balanceador de carga F5, adicione esse nó ao balanceador de carga.

   Consulte Criar um nó do F5 para cada nó de agrupamento (na página 54).

7. Se o orquestrador tiver sido configurado com um balanceador de carga do Apache, adicione esse nó ao balanceador de carga.

   a. Vá até *apache_install_location*\conf.

   b. Abra o arquivo workers.properties.

   c. Remova o comentário das seguintes linhas em Definir nó 2 no arquivo worker.properties.

      ```
      worker.node2.port=8009
      worker.node2.host=hostname
      worker.node2.type=ajp13
      worker.node2.lbfactor=1
      ```

   d. Altere *hostname* para o nome do host do servidor no qual o nó do orquestrador está sendo instalado.

   e. Adicione "node2" à linha worker.loadbalancer.balance_workers= no comportamento Load-balancing. A entrada se parece com o seguinte:

      ```
      worker.loadbalancer.balance_workers=node1,node2
      ```

      Observação: para o terceiro nó e os nós subsequentes, siga as mesmas instruções, mas substitua node2 pelo número do nó correto, por exemplo, node3 ou node4.

   f. Reinicie o Apache.

8. Se o orquestrador tiver sido configurado com um balanceador de carga NGINX, adicione esse nó ao balanceador de carga.

   a. Vá até o arquivo pam-server.conf e abra-o.

   b. Localize a linha #Define node2. (Os dados do node1 fazem referência ao primeiro nó do orquestrador; ignore as seções que se referem ao node1.)

   c. Insira os dados a seguir:

      ```
      # Define node2
        server node2_hostname:jetty_server_port max_fails=3
      fail_timeout=3s;
      }
      ```

      Observação: o valor jetty_server_port é da opção Porta do servidor, fornecido durante a instalação do primeiro nó do orquestrador de domínio. Digite 80 para a comunicação simplificada ou digite 7003 para a comunicação obsoleta.

      Dentro da tag de servidor, crie as seguintes entradas:

      ```
      Server{
           location = /ws {
      ...
      ```

```
                    // node2 is the upstream name provided above
                    proxy_pass http://node2;
                    }
          location /ws/node2/ {
                    // node2 is the upstream name provided above
                    proxy_pass http://node2;
                    }
}
```

Instalar um nó de agrupamento para um orquestrador

Os usuários com privilégios PAMAdmins podem adicionar nós de agrupamento para um orquestrador que foi instalado com um balanceador de carga.

Verifique se os pré-requisitos para instalação de um nó de agrupamento para um orquestrador (na página 204) foram atendidos. Em seguida, instale o nó de agrupamento. Esse mesmo procedimento é usado na atualização de um nó de agrupamento para uma nova release.

Siga estas etapas:

1. Efetue logon no servidor em que você planeja instalar esse nó de agrupamento para um orquestrador adicional.
2. Vá até o orquestrador ao qual deseja adicionar o nó de agrupamento e efetue logon.

   `https://nome_do_host_do_balanceador_de_carga:8443/itpam`

   `http://nome_do_host_do_balanceador_de_carga:8080/itpam`
3. Clique na guia Configuração e clique na paleta Instalação.
4. Clique em Instalar para *Instalar nó de agrupamento para o orquestrador*.
5. Se a assinatura digital não puder ser verificada, clique em Executar para iniciar a instalação.
6. Na tela Instalação de terceiros, clique em Avançar.
7. Aceite o contrato de licença e clique em Avançar.
8. Especificar o diretório de destino para instalar o nó do orquestrador e clicar em Avançar.

   O instalador criará a pasta automaticamente se ela não existir.
9. Na tela Pré-requisitos para instalação do CA Process Automation, clique em Avançar.

   Uma tela subsequente inclui a caixa de seleção a seguir:

   Usar domínio

   Especifica se esse nó de agrupamento é para o orquestrador de domínio

   Desmarcado - Especifica que esse nó de agrupamento não é para o orquestrador de domínio.

   Na tela de confirmação, clique em Avançar.
10. Clique em Concluir para prosseguir para o instalador do CA Process Automation.
11. Na tela de boas vindas, clique em Avançar.
12. Aceite o contrato de licença e clique em Avançar.

13. Especifique o diretório inicial do Java. O instalador do CA Process Automation preencherá previamente esse campo com o JDK adequado mais recente que ele foi capaz de localizar no caminho. Se necessário, vá até o diretório em que o JDK está instalado e clique em Avançar.

    O JDK é validado e a instalação do orquestrador é iniciada. Isso poderá demorar um minuto ou mais enquanto os arquivos são copiados.

14. Preencha a Tela de configuração e clique em Avançar.

    orquestrador

    Especifica o orquestrador ao qual o nó de agrupamento será adicionado. O orquestrador selecionado na lista suspensa deve ser configurado com um nome do host público que especifica o FQDN do servidor no qual o balanceador de carga está instalado.

    Nó de trabalho do balanceador de carga

    Especifica o nome do nó, por exemplo, node 2. Esse é o nome do nó especificado no arquivo workers.properties do Apache, em que *hostname* é o nome do host no qual você está instalando o nó de agrupamento:

    worker.**node2**.host=*hostname*.*mycompany*.com

    Observação: a primeira instalação do orquestrador de domínio é o node1. Para o segundo nó, digite **node2**.

15. Exiba o Nome da empresa e clique em Avançar.

16. Insira a mesma senha do certificado que foi inserida durante a instalação do orquestrador de domínio e clique em Avançar.

    Se essa senha do certificado tiver sido perdida ou esquecida, você deverá reinstalar todos os orquestradores em seu sistema, começando com o orquestrador de domínio.

17. Selecione a pasta do menu iniciar e clique em Avançar.

18. Digite as propriedades gerais para o orquestrador de domínio e clique em Avançar.

    Para obter mais informações sobre cada propriedade, consultar Instalar e configurar o orquestrador de domínio.

19. Exibir as configurações Segurança e clicar em Avançar.

20. Exibir as configurações do banco de dados e clicar em Avançar.

21. Exiba as configurações do banco de dados de geração de relatórios e clique em Avançar para concluir a instalação.

22. Clique em Concluir.

    O nó de agrupamento para o orquestrador selecionado está instalado.

Sincronizar a hora para um nó de agrupamento

Todos os nós de agrupamento para qualquer orquestrador devem ter exatamente a mesma hora do relógio, sincronizada com um servidor de tempo externo padrão. Considere uma das seguintes abordagens para sincronizar a hora de todos os nós em um agrupamento:

- Sincronize todos os orquestradores e nós de agrupamento com um servidor de tempo externo padrão (preferencial).
- Sincronize manualmente a hora de todos os nós de agrupamento adicionais, da seguinte maneira:
  1. Verifique a exatidão da hora de todos os nós de agrupamento.
  2. Execute o comando do sistema operacional apropriado em cada nó de agrupamento para sincronizar a hora de todos eles.

Capítulo 12: Ajuste do CA Process Automation

Esta seção contém os seguintes tópicos:

Como melhorar o desempenho do CA Process Automation

Conforme você aborda como aumentar ou aprimorar o desempenho, considere as seguintes diretrizes:

- Converta cada orquestrador autônomo em um agrupamento.

  Adicionar um segundo nó pode melhorar o desempenho em até 80%. A melhoria obtida depende de muitas variáveis, incluindo o conteúdo do CA Process Automation que está sendo executado.

- Conteúdo
  - Conjuntos de dados globais

    Minimize as referências aos conjuntos de dados globais, pois o acesso a eles é serializado. Isto é, apenas um objeto pode acessar um conjunto de dados de cada vez. Esta diretriz se aplica à gravações (não a leituras).

    A prática recomendada é fazer uma cópia no nível do processo dos dados necessários e, em seguida, fazer referência ao conjunto de dados do processo.

  - Processos embutidos

    Limite o uso do início de processos embutidos aos casos em que ambas as condições a seguir forem verdadeiras:

    - Há menos de 10 operadores no processo embutido.
    - O processo embutido não foi chamado dentro de um loop.

- CPU
  - Monitore o uso de CPU em todos os nós do orquestrador para determinar quais nós podem tirar maior benefício de CPU ou núcleos adicionais.
  - Adicione mais CPU ou núcleos, conforme necessário.
  - Ao executar em um ambiente virtual, dedique as CPU às VM do CA Process Automation.

- Memória
  - Ao executar em um ambiente virtual, dedique a RAM às VM do CA Process Automation.
  - Monitore o uso de memória do processo em todos os nós do orquestrador para determinar se mais RAM é necessária.

- Otimização do servidor da VM

  Consulte o fornecedor de servidor da VM para obter instruções sobre como aumentar o desempenho.

- Otimização e manutenção do banco de dados

Consulte o fornecedor de servidor de banco de dados para obter instruções sobre como aumentar e manter o desempenho do banco de dados do CA Process Automation. Essas instruções, em geral, incluem a reindexação do banco de dados, a atualização das estatísticas, bem como o monitoramento e a manutenção do sistema de arquivos no qual os dados são armazenados.

- Desativar todos os recursos desnecessários
  - Catalyst

    Caso não esteja usando os conectores do Catalyst, localize o seguinte valor no OasisConfig.properties e altere-o de verdadeiro para falso:

    ```
    # enable connector
    ucf.connector.enabled=true
    ```

  - Geração de relatórios

    Caso não esteja usando a Geração de relatórios, insira o seguinte par de chave/valor no arquivo OasisConfig.properties. As alterações feitas nesse arquivo entram em vigor quando o serviço do CA Process Automation é reiniciado.

    ```
    oasis.disable.reporting.manager=true
    ```

- VMware

  Caso esteja usando o VMware, altere a NIC virtual de E1000 para VMXNET3. Esta alteração normalmente melhora o desempenho e a confiabilidade.

Apêndice A: Usando o SiteMinder com o CA Process Automation

O CA SiteMinder fornece recursos de SSO (Single Sign-On - Logon único) em domínios de cookies simples e múltiplos, o que permite que os usuários acessem aplicativos em diferentes servidores web e plataformas ao inserir suas credenciais uma única vez em cada sessão.

Esta seção contém os seguintes tópicos:

Pré-requisitos do CA SiteMinder

Verifique se o seu sistema atende aos seguintes pré-requisitos para instalar o CA Process Automation com o CA SiteMinder:

- Um servidor do CA EEM integrado ao mesmo LDAP/AD que é usado como um diretório de usuário no servidor de diretivas do SiteMinder.
- Um agente web do CA SiteMinder integrado ao IIS ou a Apache.

Você pode usar o agente Apache do SiteMinder apenas quando houver um balanceador de carga e um orquestrador agrupado com base em Apache. Para um orquestrador autônomo, configure o encaminhamento de portas do Tomcat 8080 para a porta 80 do IIS, de forma que o agente do SM IIS funcione.

Observação: para obter mais informações, consulte o *Guia de Instalação do Agente Web do CA SiteMinder*.

Para fins de segurança, trabalhe diretamente com o administrador do CA SiteMinder para compreender e seguir todas as diretrizes existentes para o uso do CA SiteMinder por sua empresa.

Importante: é necessário reinstalar os agentes do CA Process Automation (em vez de simplesmente reiniciar) quando o URL do orquestrador de domínio é alterado. As alterações a seguir podem afetar o URL do orquestrador de domínio:

- Alteração do orquestrador de domínio de ativado para SSO para desativado para SSO.
- Alteração do orquestrador de domínio de desativado para SSO para ativado para SSO.
- Apontamento do orquestrador de domínio para um servidor de SSO diferente.

Configurar objetos do servidor de diretivas do CA SiteMinder

Para configurar o CA SiteMinder, acesse a interface de usuário administrativa do servidor de diretivas do CA SiteMinder. Para obter mais informações, consulte o *Guia de Configuração do Servidor de Diretivas do CA SiteMinder*.

Importante: antes de configurar o CA SiteMinder para o CA Process Automation, consulte o administrador do CA SiteMinder. A sua empresa pode ter diretivas estabelecidas para a seleção ou criação de domínios, convenções de nomenclatura para outras entidades ou outras considerações de segurança específicas do site.

Para configurar um objeto Agente Web para se integrar ao CA Process Automation:

1. Crie um objeto de configuração do agente na seção de infraestrutura da interface de usuário administrativa do CA SiteMinder. Selecione ApacheDefaultSettings ou IISDefaultSettings, dependendo de qual agente web os servidores web irão hospedar.
   - Navegue até a propriedade BadUrlChars do agente web e remova "/." e "//" da propriedade.
   - Navegue até a propriedade IgnoreExt e remova ".gif,.jpg,.jpeg,.png" do valor da propriedade.
   - Navegar até a propriedade LogoffUri e definir como "/itpam/Logout".
2. Crie um objeto de configuração de host. Selecione ApacheDefaultSettings ou IISDefaultSettings, dependendo de qual agente web os servidores web irão hospedar.
3. Crie um objeto de diretório na seção de infraestrutura da interface de usuário administrativa do CA SiteMinder.
4. Criar ou selecionar um domínio na seção domínio da interface administrativa do CA SiteMinder.
5. Crie uma região na seção de domínio da interface de usuário do servidor de diretivas do CA SiteMinder.
6. Na nova região, especifique o nome correto do agente, configure o filtro de recursos como "/itpam" e selecione Protegido na seção de proteção do recurso padrão.
7. Na nova região, crie uma regra com o recurso como "*" para que o recurso se pareça com web_agent/itpam* e selecione tudo na seção de ações.

   Observação: especifique essa regra na seção de diretivas adicionando-a a uma diretiva existente ou a uma nova diretiva. Para obter mais informações, consulte o *Guia de Configuração do Servidor de Diretivas do CA SiteMinder*.
8. Crie uma sub-região para cada um dos seguintes URLs e selecione Desprotegido na seção de proteção do recurso padrão:
   - /swaref.xsd
   - /genericNoSecurity
   - /images
   - /StartAgent
   - /itpamclient
   - /ServerConfigurationRequestServlet
   - /MirroringRequestProcessor
   - /soapAttachment

- /AgentConfigurationRequestServlet
- /soap
- /css
- /js

9. Crie uma diretiva na seção de diretivas e adicione a regra criada na Etapa 7 à diretiva.

   Para obter mais informações, consulte o *Guia de Configuração do Servidor de Diretivas do CA SiteMinder*.

10. (Opcional) Use os valores padrão para criar uma variável de resposta personalizada e usá-la como o parâmetro de autenticação de SSO.

    a. Crie um atributo **pamuser** de resposta personalizado do tipo WebAgent-HTTP-Header-Variable.

    b. Defina o valor da variável como o parâmetro usado para a ID do usuário LDAP/ActiveDirectory.

    c. Adicione essa resposta personalizada à regra mencionada na Etapa 9.

       Observação: durante a instalação do CA Process Automation, especifique o parâmetro **pamuser** do cabeçalho como o Parâmetro de autenticação de SSO com o Tipo de autenticação de SSO como **Cabeçalho**. Para obter mais informações, consulte o *Guia de Configuração do Servidor de Diretivas do CA SiteMinder*.

Integrar o CA Process Automation com o IIS para Single Sign-On

Observação: para integrar o CA SiteMinder ao agrupamento, selecione o agente do Apache SiteMinder.

Para configurar o Single Sign-On com IIS

1. Faça com que o administrador do CA SiteMinder instale o agente web do CA SiteMinder em um computador que tenha o IIS instalado.
2. Se o IIS estiver configurado para SSL, descompacte IIS_https_httpfolders.zip da pasta /SSO/IIS da mídia de pré-requisitos de terceiros do CA Process Automation no diretório inicial do site em ao qual o CA SiteMinder está integrado.

3. Verifique se as seguintes pastas foram criadas no diretório inicial:
   - c2orepository +
   - itpam
   - mirroringrepository
4. Abra o Gerenciador IIS e remova o modo SSL nas seguintes pastas:

   No site:

   - c2orepository
   - mirroringrepository

   Na pasta itpam:

   - MirroringRequestProcessor
   - StartAgent
   - genericNoSecurity

   Para remover o modo SSL:

   a. Abra as propriedades da pasta correspondente.

   b. Selecione a guia Segurança de diretório e, em seguida, clique em Editar na seção de comunicação segura e desmarque a caixa de seleção Exigir SSL.

   Observação: para integrar o CA Process Automation, use o filtro "redirecionador do Tomcat" quando o agente web do CA SiteMinder estiver implantado no IIS.

Como configurar o IIS para redirecionar para o Tomcat

Pré-requisito

O agente do CA SiteMinder deve estar em execução no mesmo servidor do IIS antes de o redirecionador do Tomcat ser configurado para redirecionar as solicitações para o CA Process Automation. Para obter mais informações, consulte o *Guia de Instalação do CA SiteMinder*.

Siga estas etapas:

1. Verifique se o servidor web do IIS está instalado e em execução corretamente.
2. Copie a pasta TomcatRedirector no computador em que o IIS está instalado, de preferência no seguinte caminho:

   ```
   C:\Arquivos de programas\CA\SharedComponents
   ```

3. Edite o arquivo isapi_redirect.properties da pasta bin para refletir o caminho correto, se ele for diferente.

   Exemplo:

   ```
   # Configuration file for the Jakarta ISAPI Redirector
   # The path to the ISAPI Redirector Extension, relative to the
   website
   # This must be in a virtual directory with execute privileges.
   extension_uri=/TomcatRedirector/isapi_redirect.dll
   ```

   Observação: TomcatRedirector é o nome do diretório virtual.

   ```
   # Full path to the log file for the ISAPI Redirector
   log_file=C:\Program
   Files\CA\SharedComponents\TomcatRedirector\logs\isapi_redirect.
   log
   # Log level (debug, info, warn, error or trace)
   log_level=error
   # Full path to the workers.properties file
   worker_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\workers.propert
   ies
   # Full path to the uriworkermap.properties file\
   worker_mount_file=c:\Program
   Files\CA\SharedComponents\TomcatRedirector\conf\uriworkermap.pr
   operties
   ```

4. Edite o nome do host no arquivo TomcatRedirector\conf\workers.properties para refletir o nome do host correto. Substitua as referências por localhost.

   Exemplo:

   ```
   # statement and uncomment the three worker.ajp13w01 lines
   ##################################################################
   #######
   # The workers that jk should create and work with
   worker.list=ajp13w01
   # Defining a worker named ajp13w01 and of type ajp13
   # Note that the name and the type do not have to match.
   worker.ajp13w01.type=ajp13
   worker.ajp13w01.host=pa-w2k3
   worker.ajp13w01.port=8009
   ```

   Observação: no código anterior, pa-w2k3 é o computador no qual o CA Process Automation está instalado.

5. Abra o console do Gerenciador do IIS.

6. Clique com o botão direito do mouse no site padrão, escolha o novo diretório virtual e faça referência à pasta TomcatRedirector\bin criada na Etapa 4.

7. Navegue até a pasta TomcatRedirector\logs no Windows Explorer e conceda todas as permissões para o arquivo de log nessa pasta para o usuário do serviço de rede.

8. Clique com o botão direito do mouse no diretório virtual e selecione as propriedades, clique em Criar ao lado do nome do aplicativo, selecione Scripts e executáveis para as permissões de execução e clique em OK.

   Observação: verifique se o valor de Nome de aplicativo é igual ao do Nome do diretório virtual fornecido no arquivo isapi_redirect.properties (Etapa 3).

   a. Clique com o botão direito do mouse nas extensões de serviço web, nomeie-as como TomcatRedirector e selecione o caminho para o arquivo TomcatRedirector\bin\isapi_redirect.dll a fim de adicionar uma extensão de serviço web. Selecione a opção de Definir status da extensão como permitido.

   b. Recicle o Serviço de administração do IIS.

9. Adicione o isapi_redirect.dll como um filtro ISAPI em seu site do IIS. Abra o Gerenciador do IIS e clique com o botão direito do mouse na pasta Sites para abrir a caixa de diálogo de propriedades de todos os sites; selecione a guia Filtro ISAPI, clique em Adicionar e selecione o isapi_redirect.dll como executável.

10. Verifique se as solicitações estão sendo encaminhadas para o Tomcat acessando http://localhost:80.

Integre o CA Process Automation com o Apache para SSO

Para configurar o Single Sign-On com o Apache

1. Faça seu administrador do CA SiteMinder instalar o WebAgent do CA SiteMinder em uma máquina que tenha o Apache instalado.
2. Configure o Apache com as configurações de Host público. Para obter mais informações, consulte Instalar o orquestrador de domínio (na página 96).

   Observação: entre em contato com o administrador do CA SiteMinder para obter mais detalhes.

Ativar logoff no CA Process Automation para SSO

Você pode permitir o logoff com Single Sign-on no CA Process Automation.

Siga estas etapas:

1. Navegue até o seguinte local:

   install_dir/server/c2o/.config

2. Clique duas vezes para abrir o arquivo OasisConfig.properties.
3. Modifique ALLOW_SSO_LOGOUT para verdadeiro.

Apêndice B: Portas usadas pelo CA Process Automation

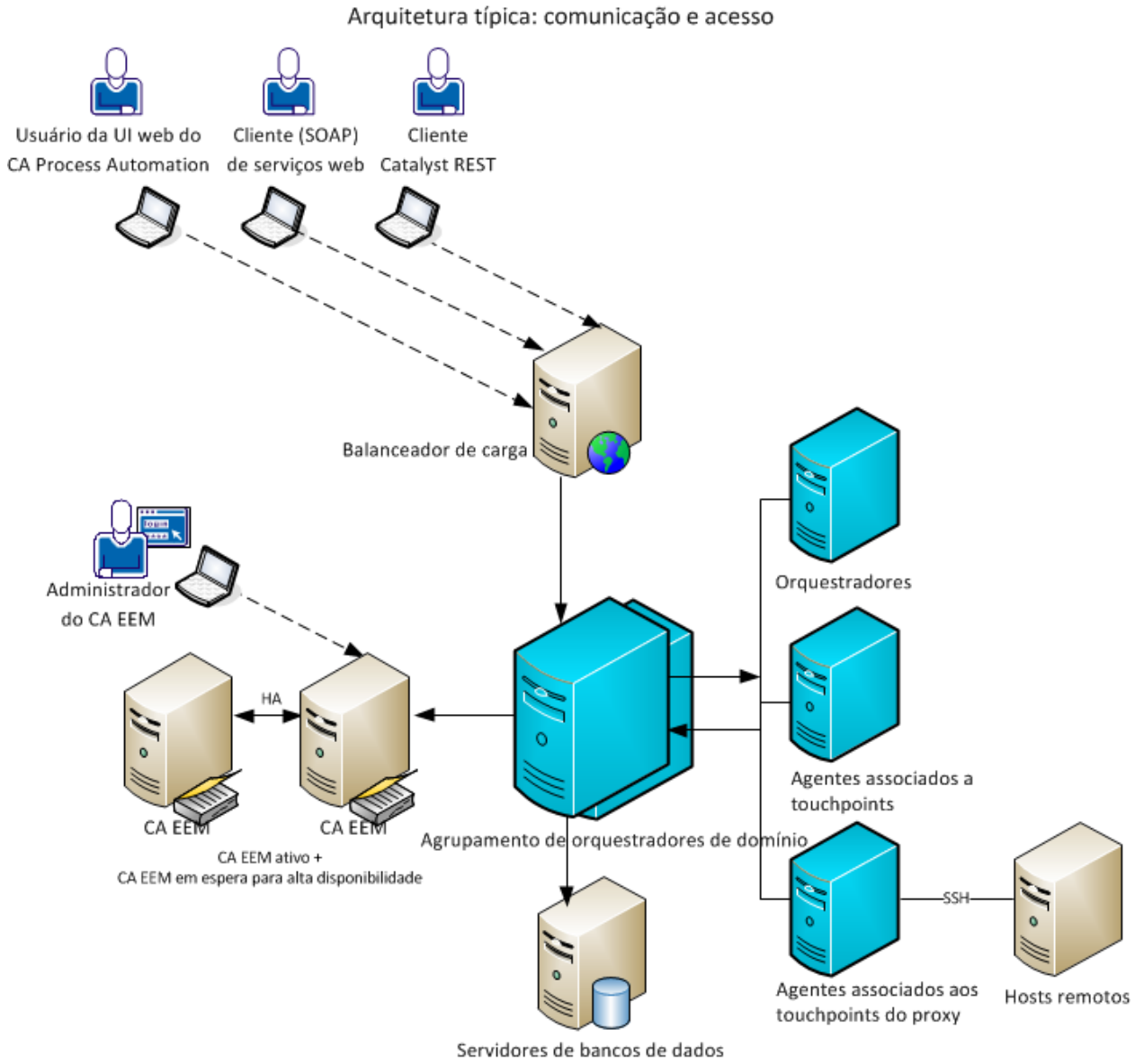
Este apêndice é composto de tabelas que descrevem em detalhes o uso de portas dos vários componentes do CA Process Automation. Essas tabelas são abrangentes e contêm duplicação para fornecer uma visão completa de cada componente.

Para obter uma ilustração de como os componentes se comunicam, consulte o tópico Comunicação em uma arquitetura típica (na página 224).

Esta seção contém os seguintes tópicos:

Comunicação em uma arquitetura típica

O diagrama a seguir mostra as relações entre os componentes referenciados neste apêndice sobre as portas usadas pelo CA Process Automation.



Mais informações:

Planejando os locais dos componentes de suporte (na página 67)

Portas usadas pelo CA EEM

As tabelas a seguir fornecem uma visão geral das portas usadas para as comunicações de e para o CA EEM (CA Embedded Entitlements Manager).

Comunicação do CA EEM

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
CA EEM	Qualquer	CA EEM	509	TCP	Configuração do CA EEM	Usada pelo CA EEM iTechPoz quando o CA EEM estiver configurado como um agrupamento de HA (High Availability - Alta Disponibilidade).
CA EEM	Qualquer	CA EEM	1684	TCP	Configuração do CA EEM	Usada pelo CA EEM iTechPoz Router quando o CA EEM estiver configurado como um agrupamento de HA (CA EEM 8.4 somente).
CA EEM	Qualquer	CA EEM	5250	TCP	Configuração do CA EEM	Usada pelo CA EEM iGateway quando o CA EEM estiver configurado como um agrupamento de HA.

Comunicação para o CA EEM

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
CA EEM	Qualquer	CA EEM	509	TCP	Configuração do CA EEM	Usada pelo CA EEM iTechPoz quando o CA EEM estiver configurado como um agrupamento de HA (High Availability - Alta Disponibilidade).

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
CA EEM	Qualquer	CA EEM	1684	TCP	Configuração do CA EEM	Usada pelo CA EEM iTechPoz Router quando o CA EEM estiver configurado como um agrupamento de HA (CA EEM 8.4 somente).
CA EEM	Qualquer	CA EEM	5250	TCP	Configuração do CA EEM	Usada pelo CA EEM iGateway quando o CA EEM estiver configurado como um agrupamento de HA.
orquestrador	Qualquer	CA EEM	5250	TCP	Configuração do CA EEM	Usada pelo CA EEM iGateway.
Navegador web (Administrador do CA EEM)	Qualquer	CA EEM	5250	TCP	Configuração do CA EEM	Navegador web que acessa a interface de usuário do CA EEM.

Portas usadas pelo balanceador de carga

As tabelas a seguir fornecem uma visão geral das portas que são usadas para as comunicações de e para o balanceador de carga configurado. Os balanceadores de carga suportados incluem o NGINX, o Apache e o F5. As portas incluem aquelas para Jboss@Orchestrator e para Jetty@Orchestrator.

Comunicação do balanceador de carga

Observação: as portas ouvintes de um balanceador de carga podem ser configuradas no arquivo observado na coluna Configuração. A documentação de cada balanceador de carga contém o local de cada arquivo de configuração.

Apache

httpd.conf

tomcat.connector.ajp.port

NGINX

pam-server.conf

secure-pam-server.conf

pam-rest.conf

F5

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Balanceador de carga	Qualquer	orquestrador	80	HTTP	httpd.conf	O balanceador de carga se comunica com o orquestrador nesta porta. Esta porta não se aplica ao NGINX.
Balanceador de carga	Qualquer	orquestrador	443	HTTPS	httpd.conf	O balanceador de carga se comunica com orquestradores seguros nesta porta. Esta porta não se aplica ao NGINX.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Balanceador de carga	Qualquer	orquestrador	8010	TCP/AJP	tomcat.connector.ajp.port	Loadbalancer - Porta do conector AJP entre o balanceador de carga e o orquestrador. Esta porta não se aplica ao NGINX.
Balanceador de carga	Qualquer	orquestrador	8080	HTTP	httpd.conf, pam-server.conf	O balanceador de carga se comunica com o orquestrador nesta porta.
Balanceador de carga	Qualquer	orquestrador	8443	HTTPS	httpd.conf, secure-pam-server.conf	O balanceador de carga se comunica com orquestradores seguros nesta porta.
Balanceador de carga	Qualquer	orquestrador	8009	TCP/AJP	tomcat.connector.ajp.port	Loadbalancer - Porta do conector AJP entre o balanceador de carga e o orquestrador. Esta porta não se aplica ao NGINX.
Balanceador de carga	Qualquer	orquestrador	7000	HTTP	node0-config.xml, http.port, pam-rest.conf	Porta do recipiente do Catalyst do CA Process Automation.
Balanceador de carga	Qualquer	orquestrador	7443	HTTPS	node0-config.xml, https.port, pam-rest.conf	Porta segura do recipiente do Catalyst do CA Process Automation.

Comunicação para o balanceador de carga

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Cliente do Catalyst REST	Qualquer	Balanceador de carga	7000	HTTP	node0-config.xml, http.port, pam-rest.conf	Porta do recipiente do Catalyst do CA Process Automation.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Cliente do Catalyst REST	Qualquer	Balanceador de carga	7443	HTTPS	node0-config.xml, https.port, pam-rest.conf	Porta segura do recipiente do Catalyst do CA Process Automation.
Agente	Qualquer	Balanceador de carga	80	HTTP	httpd.conf	Porta do balanceador de carga para uma comunicação básica.
Agente	Qualquer	Balanceador de carga	443	HTTPS	httpd.conf	Porta do balanceador de carga para uma comunicação segura.
Navegador web (Usuário do CA Process Automation)	Qualquer	Balanceador de carga	80	TCP	httpd.conf	Porta do balanceador de carga para uma comunicação básica.
Navegador web (Usuário do CA Process Automation)	Qualquer	Balanceador de carga	443	TCP	httpd.conf	Porta do balanceador de carga para uma comunicação segura.
Cliente do serviço web (SOAP)	Qualquer	Balanceador de carga	80	TCP	httpd.conf	Porta do balanceador de carga para uma comunicação básica.
Cliente do serviço web (SOAP)	Qualquer	Balanceador de carga	443	TCP	httpd.conf	Porta do balanceador de carga para uma comunicação segura.

Portas usadas por um orquestrador

As tabelas a seguir fornecem uma visão geral das portas usadas para comunicações, especificamente:

- Comunicação de um orquestrador para outro componente em um sistema do CA Process Automation.
- Comunicação entre orquestradores.
- Comunicação para um orquestrador de outro componente em um sistema do CA Process Automation.

Comunicação de um orquestrador para outro componente

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	CA EEM	5250	TCP	Configuração do CA EEM	Usada pelo CA EEM iGateway.
orquestrador	Qualquer	Agente	7003	HTTP/HTTPS	Script de instalação do agente	**Depreciado** O agente escuta nesta porta obsoleta ao usar o modo de comunicação antigo com os orquestradores.
orquestrador	Qualquer	Servidor de banco de dados Microsoft SQL	1433	TCP	Microsoft SQL configurado	A porta do banco de dados pode ser alterada na instalação do servidor de banco de dados; 1433 é o valor padrão.
orquestrador	Qualquer	Servidor de banco de dados MySQL	3306	TCP	MySQL configurado	A porta do banco de dados pode ser alterada na instalação do servidor de banco de dados; 3306 é o valor padrão.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	Servidor de bancos de dados Oracle	1521	TCP	Escuta configurada para Oracle	A porta do banco de dados pode ser alterada ao criar a escuta; 1521 é o valor padrão para a porta de escuta do Oracle. A instância do banco de dados pode ser associada a uma escuta diferente. Consulte a configuração do Oracle.
orquestrador	Qualquer	Host remoto de destino	22	TCP	Porta SSH padrão	Usada para a comunicação SSH com um touchpoint do proxy ou um grupo de hosts.

Comunicação entre os orquestradores de domínio e os orquestradores que não são de domínio

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Orquestrador de domínio	Qualquer	Orquestrador que não é de domínio	1090	TCP	jboss.remoting.port	A porta de comunicação remota do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	1098	TCP	jboss.rmi.port	A porta RMI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	1099	TCP	jboss.jndi.port	A porta JNDI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	1100	TCP	jboss.ha.jndi.port	JBoss: a nomenclatura do Java de HA e a interface de diretório são usadas apenas entre os orquestradores.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	Orquestrador que não é de domínio	1101	TCP	jboss.ha.jndi.port	JBoss: a invocação de método remoto do Java de HA é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	1102	UDP	jboss.mcast.jndi.autodiscovery.port	JBoss: o serviço de detecção automática de JNDI é usado apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	3873	TCP	jboss.remoting.transport.Connector.port	JBoss: o conector de comunicação remota de EJB3 é usado apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	4444	TCP	jboss.rmi.object.port	A porta do servidor RMI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	4445	TCP	jboss.ha.pooledinvoker.serverbind.port	A porta do chamador em pool do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	4446	TCP	jboss.pooledinvoker.serverbind.port	A porta do chamador em pool do JBoss de HA é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	4447	TCP	jboss.ha.rmi.object.port	A porta do servidor HA-RMI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	4448	TCP		A porta do chamador em pool do JBoss de HA é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	4457	TCP	jboss.service.binding.port	A porta de mensagens do JBoss é usada apenas entre os orquestradores.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	Orquestrador que não é de domínio	4712	TCP	jboss.tx.recovery.manager.port	A porta de gerente de recuperação do status da transação do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	4713	TCP		A porta de gerente do status da transação do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	7001	HTTP/HTTPS	oasis.jxta.port	Porta usada para a comunicação entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	7600	TCP	jboss.jgroups.tcp.tcp_port	A porta de agrupamento do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	7900	TCP	jboss.messaging.datachanneltcpport	A porta de agrupamento do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	7901	TCP	jboss.messaging.controlchanneltcpport	A porta de agrupamento do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	8083	TCP	jboss.rmi.classloader.webservice.port	A porta do serviço web RMI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	Orquestrador que não é de domínio	8080			
orquestrador	Qualquer	Orquestrador que não é de domínio	8443			
orquestrador	Qualquer	Orquestrador que não é de domínio				

Comunicação entre os nós do orquestrador agrupado

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	orquestrador	1090	TCP	jboss.remoting.port	A porta de comunicação remota do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	1098	TCP	jboss.rmi.port	A porta RMI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	1099	TCP	jboss.jndi.port	A porta JNDI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	1100	TCP	jboss.ha.jndi.port	JBoss: a nomenclatura do Java de HA e a interface de diretório são usadas apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	1101	TCP	jboss.ha.jndi.port	JBoss: a invocação de método remoto do Java de HA é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	1102	UDP	jboss.mcast.jndi.autodiscovery.port	JBoss: o serviço de detecção automática de JNDI é usado apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	3873	TCP	jboss.remoting.transport.Connector.port	JBoss: o conector de comunicação remota de EJB3 é usado apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	4444	TCP	jboss.rmi.object.port	A porta do servidor RMI do JBoss é usada apenas entre os orquestradores.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	orquestrador	4445	TCP	jboss.ha.pooledinvoker.serverbind.port	A porta do chamador em pool do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	4446	TCP	jboss.pooledinvoker.serverbind.port	A porta do chamador em pool do JBoss de HA é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	4447	TCP	jboss.ha.rmi.object.port	A porta do servidor HA-RMI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	4448	TCP		A porta do chamador em pool do JBoss de HA é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	4457	TCP	jboss.service.binding.port	A porta de mensagens do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	4712	TCP	jboss.tx.recovery.manager.port	A porta de gerente de recuperação do status da transação do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	4713	TCP		A porta de gerente do status da transação do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	7001	HTTP/HTTPS	oasis.jxta.port	Porta usada para a comunicação entre os orquestradores.
orquestrador	Qualquer	orquestrador	7600	TCP	jboss.jgroups.tcp.tcp_port	A porta de agrupamento do JBoss é usada apenas entre os orquestradores.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	orquestrador	7900	TCP	jboss.messaging.datachannelteppport	A porta de agrupamento do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	7901	TCP	jboss.messaging.controlchanneltcpport	A porta de agrupamento do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	8083	TCP	jboss.rmi.classloader.webservice.port	A porta do serviço web RMI do JBoss é usada apenas entre os orquestradores.
orquestrador	Qualquer	orquestrador	61618			ActiveMQ...

Observação: o CA Process Automation utiliza o JBoss 5.1. Por sua vez, o JBoss 5.1 usa portas dinâmicas intermitentes no intervalo (49152-65535) quando configurado como um agrupamento para comunicação entre nós (apenas orquestradores). Muitas das portas são usadas para gerenciamento dentro do agrupamento. A CA não recomenda a divisão de agrupamentos entre links WAN/firewalls. A configuração padrão do agrupamento usa multitransmissão, e se a comunicação de multitransmissão não estiver aberta de ponta a ponta entre os nós do agrupamento, esses nós não farão efetivamente parte do mesmo agrupamento, gerando um comportamento imprevisível.

Comunicação com um orquestrador agrupado de outro componente

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Balanceador de carga	Qualquer	orquestrador	8080	HTTP	httpd.conf do Apache	O balanceador de carga do Apache comunica-se com os orquestradores nesta porta.
Balanceador de carga	Qualquer	orquestrador	8443	HTTPS	httpd.conf do Apache	O balanceador de carga do Apache comunica-se com orquestradores seguros nesta porta.
Balanceador de carga	Qualquer	orquestrador	7000	HTTP	node0-config.xml, http.port	Porta do recipiente do Catalyst do CA Process Automation.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Balanceador de carga	Qualquer	orquestrador	7443	HTTPS	node0-config.xml, https.port	Porta segura do recipiente do Catalyst do CA Process Automation.
Balanceador de carga	Qualquer	orquestrador	8009	TCP/AJP	tomcat.connector.ajp.port	Loadbalancer - Porta do conector AJP entre o balanceador de carga e o orquestrador.
Agente	Qualquer	orquestrador	8080	HTTP	tomcat.connector.http.port	Somente comunicações obsoletas.
Agente	Qualquer	orquestrador	8443	HTTPS	tomcat.secure.port	Somente comunicações obsoletas.
Agente	Qualquer	orquestrador	7001	HTTP/HTTPS	oasis.jxta.port	Porta obsoleta

Comunicação com um orquestrador não agrupado de outro componente

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Agente	Qualquer	orquestrador	8080	HTTP	tomcat.connector.http.port	Interface de usuário do CA Process Automation - Porta básica.
Agente	Qualquer	orquestrador	8443	HTTPS	tomcat.secure.port	Interface de usuário do CA Process Automation - Porta segura.

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Agente	Qualquer	orquestrador	7001	HTTP/HTTPS	oasis.jxta.port	Porta obsoleta
orquestrador	Qualquer	Agente	80	HTPP	Jetty	Conexão de soquete da web estabelecida por agentes.
orquestrador	Qualquer	Agente	443	HTTPS	Jetty	Conexão de soquete da web estabelecida por agentes.

Portas usadas por um agente

As tabelas a seguir fornecem uma visão geral das portas usadas para as comunicações de e para um agente do CA Process Automation.

Comunicação de um agente

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Agente	Qualquer	orquestrador	8080	HTTP	tomcat.connector.http.port	Interface de usuário do CA Process Automation - Porta para comunicações básicas.
Agente	Qualquer	orquestrador	8443	HTTPS	tomcat.secure.port	Interface de usuário do CA Process Automation - Porta para comunicações seguras.
Agente	Qualquer	Balanceador de carga do Apache	80	HTTP	httpd.conf do Apache	Porta do balanceador de carga do Apache para uma comunicação básica.
Agente	Qualquer	Balanceador de carga do Apache	443	HTTPS	httpd.conf do Apache	Porta do balanceador de carga do Apache para uma comunicação segura.
Agente	Qualquer	orquestrador	7001	HTTP/HTTPS	oasis.jxta.port	Porta do servidor obsoleta

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Agente	Qualquer	orquestrador	80	HTTP	Jetty	Porta do servidor
Agente	Qualquer	orquestrador	443	HTTPS	Jetty	Porta do servidor
Agente	Qualquer	Host remoto de destino	22	TCP	Porta SSH padrão	Usada para a comunicação SSH com um touchpoint do proxy ou um grupo de hosts.

Comunicação para um agente

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	Agente	7003	HTTP/HTTPS	Script de instalação do agente	O agente escutava nesta porta obsoleta por comunicação com os orquestradores.
orquestrador	Qualquer	Agente	80	HTTP	Jetty	Conexão de soquete da web estabelecida por agentes.
orquestrador	Qualquer	Agente	443	HTTPS	Jetty	Conexão de soquete da web estabelecida por agentes.

Portas usadas por servidores de banco de dados

A tabela a seguir fornece uma visão geral das portas usadas para as comunicações para um servidor de banco de dados.

Comunicação para um servidor de banco de dados

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
orquestrador	Qualquer	Servidor de banco de dados Microsoft SQL	1433	TCP	Microsoft SQL configurado	A porta do banco de dados pode ser alterada na instalação do servidor de banco de dados; 1433 é o valor padrão.
orquestrador	Qualquer	Servidor de banco de dados MySQL	3306	TCP	MySQL configurado	A porta do banco de dados pode ser alterada na instalação do servidor de banco de dados; 3306 é o valor padrão.
orquestrador	Qualquer	Servidor de bancos de dados Oracle	1521	TCP	Escuta configurada para Oracle	A porta do banco de dados pode ser alterada ao criar a escuta; 1521 é o valor padrão para a porta de escuta do Oracle. A instância do banco de dados pode ser associada a uma escuta diferente. Consulte a configuração do Oracle.

Portas usadas por clientes web

A tabela a seguir fornece uma visão geral das portas usadas para as comunicações de clientes web.

Comunicação de clientes web

De	Porta	Para	Porta de escuta padrão	Protocolo	Configuração	Descrição
Navegador web (Administrador do CA EEM)	Qualquer	CA EEM	5250	TCP	Configuração do CA EEM	Navegador web que acessa a interface de usuário do CA EEM.
Navegador web (Usuário do CA Process Automation)	Qualquer	Balanceador de carga do Apache	80	TCP	httpd.conf do Apache	Porta do balanceador de carga do Apache para uma comunicação básica.
Navegador web (Usuário do CA Process Automation)	Qualquer	Balanceador de carga do Apache	443	TCP	httpd.conf do Apache	Porta do balanceador de carga do Apache para uma comunicação segura.
Cliente de serviços web (SOAP)	Qualquer	Balanceador de carga do Apache	80	TCP	httpd.conf do Apache	Porta do balanceador de carga do Apache para uma comunicação básica.
Cliente de serviços web (SOAP)	Qualquer	Balanceador de carga do Apache	443	TCP	httpd.conf do Apache	Porta do balanceador de carga do Apache para uma comunicação segura.
Cliente do Catalyst REST	Qualquer	Balanceador de carga do Apache	7000	HTTP	node0-config.xml, http.port	Porta do recipiente do Catalyst do CA Process Automation.
Cliente do Catalyst REST	Qualquer	Balanceador de carga do Apache	7443	HTTPS	node0-config.xml, https.port	Porta segura do recipiente do Catalyst do CA Process Automation.
Navegador web (Administrador do CA Catalyst)	Qualquer	orquestrador	8181	TCP	ucf.pax.web.http.port	Interface de usuário administrativa do Catalyst Karaf - não usada em operações comuns.

Apêndice C: Manter o nome DNS ou endereço IP do orquestrador

Esta seção contém os seguintes tópicos:

Manter endereços IP

Talvez haja a necessidade de manter endereços IP ou nomes. Os exemplos estão a seguir:

- Altere o endereço IP e o nome de um orquestrador.

  Modifique a combinação de nome e endereço IP sempre que eles aparecerem nos arquivos a seguir.

  install_dir/server/c2o/.config/OasisConfig.properties

  install_dir/server/c2o/.config/Domain.xml

  Observação: para continuar usando o mesmo nome do host em todas as referências do CA Process Automation, modifique o DNS com o novo endereço IP.

- Se você instalar agentes usando endereços IP que se alteram, reconfigure o agente atualizando o seguinte arquivo:

  install_dir/PAM Agent/PAMAgent/.config/OasisConfig.properties

  Altere o valor da seguinte propriedade:

  oasis.jxta.host

- Use vários endereços IP para o CA Process Automation quando tiver dois NICs, um interno e outro externo.

  Para que o CA Process Automation seja associado no endereço IP externo, adicione a seguinte propriedade ao OasisConfig.properties:

  jboss.bind.address=*xxx.xxx.xxx.xxx*

Resolver caractere inválido no nome DNS do CA Process Automation

Na release 3.1, o CA Process Automation aceita a instalação de orquestradores com nomes DNS contendo caracteres restritos, como sublinhados (_).

Se tiver instalado um orquestrador com um nome de host inválido, você deverá executar as seguintes ações corretivas:

1. Criar um registro DNS que mapeia o nome do host correto para seu endereço IP.

   Consulte o tópico Sintaxe de nomes de host DNS (na página 246) para obter os padrões.

2. Criar um registro DNS que mapeia o nome incorreto para o nome correto.

   Consulte o tópico Ativar o DNS para resolver um nome de host inválido (na página 244).

3. Atualizar o arquivo OasisConfig.properties com o nome correto.

   Consulte o tópico Manter o nome de host DNS (na página 245).

Ativar o DNS para resolver um nome de host inválido

Se tiver criado um orquestrador com um nome de host que inclui um sublinhado ou outro caractere inválido, você pode tomar medidas que permitem que o servidor DNS resolva o endereço IP correto de um nome de host inválido. Isso exige que você crie dois registros no servidor DNS. O primeiro registro informa que o nome inválido original é um alias de outro nome canônico.

Siga estas etapas:

1. No Sistema de Nome de Domínio, crie um registro canônico com um nome de host novo e válido.
2. Crie um registro CNAME que mapeia o nome canônico para o nome inválido original.

Nome	Tipo	Valor
my_host.mycompany.com.	CNAME	myhost.mycompany.com.
myhost.mycompany.com	A	172.24.36.107

Nesse exemplo, my_host.mycompany.com é um alias para o nome canônico (CNAME) myhost.mycompany.com.

Quando o resolvedor DNS encontrar um registro CNAME ao consultar o registro de recurso original, ele reiniciará a consulta usando o CNAME em vez do nome original. O nome canônico apontado por um registro CNAME pode estar em qualquer lugar no DNS.

Manter o nome de host DNS

É possível modificar o nome de host para um orquestrador. Por exemplo, se o nome de host não estiver de acordo com a sintaxe com suporte, você poderá atualizá-lo. Se você tiver instalado o CA Process Automation usando um nome de host DNS inválido contendo caracteres restritos, como sublinhados, crie um alias que esteja de acordo com os padrões de DNS. Em seguida, substitua manualmente o nome de host inválido por esse alias no arquivo OasisConfig.properties.

Siga estas etapas:

1. Crie um alias. Consulte o tópico Ativar o DNS para resolver um nome de host inválido (na página 244).
2. Efetue logon como administrador no servidor em que o orquestrador de domínio está instalado.
3. Vá até a seguinte pasta, em que install_dir faz referência ao caminho em que o orquestrador de domínio está instalado:

   install_dir/server/c2o/.config
4. Abra o arquivo OasisConfig.properties com um editor.
5. Use Localizar para encontrar a seguinte propriedade:

   oasis.local.hostname
6. Altere o valor da propriedade oasis.local.hostname=.
7. Salve o arquivo e saia.
8. Reinicie o serviço do orquestrador.
   a. Interrompa o orquestrador (na página 137).
   b. Inicie o orquestrador (na página 138).

Sintaxe de nomes de host DNS

Há muitos locais onde você pode digitar um FQDN ou um endereço IP. Se os nomes de host DNS incluírem um caractere sublinhado ou, de qualquer maneira, não estiverem de acordo com a sintaxe exigida, especifique o endereço IP.

Os nomes de host DNS válidos:

- Começam com um caractere alfabético.
- Terminam com um caractere alfanumérico.
- Contém de 2 a 24 caracteres alfanuméricos.
- Podem conter o caractere especial de sinal de subtração (-).

  Importante: o sinal de subtração (-) é o único caractere especial válido permitido em nomes de hosts DNS.

Apêndice D: Solução de problemas

Esta seção descreve os métodos de resolução de problemas para usar o CA Process Automation.

Esta seção contém os seguintes tópicos:

Falha na instalação do CA Process Automation

Sintoma:

Se uma tentativa inicial de instalar o CA Process Automation falhar, tentativas subsequentes para a instalação do CA Process Automation no mesmo local também falharão.

Solução:

Para reinstalar o CA Process Automation, limpe as entradas de registro, arquivos e pastas restantes do local em questão antes de iniciar a instalação ou use um local diferente.

Possível problema ao executar o CA Process Automation em um servidor da VMWare usando a interface de rede E1000

Sintoma:

As principais causas desse problema são falhas raras e esporádicas de E/S de soquete, que podem fazer com que o software de chamada aguarde indefinidamente pela conclusão de uma leitura.

Da perspectiva dos usuários, o sintoma mais típico seria a suspensão inesperada de processos que normalmente são concluídos sem problemas, e que são retomados e concluídos como esperado após a reinicialização do orquestrador do CA Process Automation. Isso pode afetar um pequeno subconjunto de processos ou todos os processos em execução. Não tem correlação com o tempo de atividade do orquestrador e talvez se manifeste pouco depois de uma reinicialização, ou após dias, semanas ou meses de funcionalidade sem falhas do orquestrador.

Esse problema só foi visto em ambientes que executam altos volumes de processos do CA Process Automation. Na maioria dos ambientes onde o E1000 NIC está instalado, o problema nunca ocorreu ou ocorre com uma frequência tão baixa que não foi detectado.

Solução:

Esse problema é muito difícil de ser confirmado. Se esse problema ocorrer, geralmente o thread do CA Process Automation está parado em uma leitura do socket e nenhum erro relevante é gravado nos arquivos de log; a confirmação do problema exige a revisão de uma série de despejos de thread do Java executados durante uma ocorrência deste problema para confirmar se o operador está parado em uma leitura do socket.

Quando erros relacionados a esse problema são observados, geralmente indicam erros de conexão genéricos, que poderiam ter outras causas legítimas e não relacionadas. A seguir está um exemplo:

```
2013-07-24 18:55:23.219 WARN  [org.hibernate.jdbc.AbstractBatcher]
[nPool Worker-23] exception clearing maxRows/queryTimeout
com.microsoft.sqlserver.jdbc.SQLServerException: The connection is
closed.
                at
com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverErro
r(Unknown Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerConnection.checkClosed(Unkno
wn Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.checkClosed(Unknow
n Source)
                at
com.microsoft.sqlserver.jdbc.SQLServerStatement.getMaxRows(Unknown
Source)
```

```
                at
org.jboss.resource.adapter.jdbc.CachedPreparedStatement.getMaxRows
(CachedPreparedStatement.java:367)
                at
org.jboss.resource.adapter.jdbc.WrappedStatement.getMaxRows(Wrappe
dStatement.java:378)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:272)
                at
org.hibernate.jdbc.AbstractBatcher.closeQueryStatement(AbstractBat
cher.java:209)
```

. . . e assim por diante.

Nesses casos, a identificação do problema exige testes, e outros motivos de falha de comunicação devem ser excluídos.

Falhas do processo frequentes ou uma falha repetida de um operador individual ou de vários operadores provavelmente indicam outros problemas não relacionados na criação do processo ou na funcionalidade do orquestrador.

Em sites onde este problema foi confirmado, a reconfiguração do servidor da VMWare de um driver de placa de interface de rede E1000 para um driver VMXnet-3 NIC parece ser uma mitigação muito eficiente.

A CA Technologies evita declarar que esta é uma resolução completa, uma vez que a taxa de incidente é muito rara e o período entre as ocorrências, mesmo com o E1000 NIC, pode ser muito longo.

Se a verificação da ocorrência for necessária antes de fazer essa alteração, entre em contato com o Suporte para obter assistência para configurar o sistema de log e os despejos de thread do Java necessários para solucionar problemas e verificar esta ocorrência em particular.

Oracle Bug nº 9347941

Importante: Ao executar com versões do Oracle RDBMS anteriores ao release 11.1.0.7, o CA Process Automation pode, ocasionalmente, enfrentar o defeito 9347941 conhecido do Oracle RDBMS, no qual inserções simultâneas de dados CLOB, em que os valores de cada coluna excedem 52.000 bytes de tamanho, podem, às vezes, fazer com que essas colunas sejam atualizadas de maneira incorreta com a substituição dos dados excedentes por espaços. Esse problema foi encontrado na utilização das versões 10g e anteriores à 11g do Oracle RDBMS.

Sintoma:

O processo do CA Process Automation pode ficar parado. É necessário redefinir o processo no operador correspondente no qual o processo está parado para continuar a execução do processo até a conclusão. Esse problema não é frequente e ocorre somente com taxas extremamente altas de contenção de atualização.

Solução:

Isso não foi verificado durante a execução da versão 11.1.0.7 ou 11.2.0.2 do Oracle, e recomenda-se que os sites que utilizam o Oracle para seus bancos de dados do CA Process Automation executem a versão 11.1.0.7, 11.2.0.2 ou posterior.

Limitações do Internet Explorer

O Internet Explorer limita a instalação do agente em uma rede diferente daquela em que o orquestrador de domínio está instalado.

Sintoma:

Acesse o orquestrador de domínio usando o Internet Explorer e instale o agente do CA Process Automation em uma rede diferente daquela em que o orquestrador de domínio está instalado. A instalação pode falhar ao baixar os arquivos JAR para instalação.

Solução:

Uma possível causa desse problema esporádico pode ser que o Java não possa carregar arquivos JAR enquanto estiver roteando por meio do proxy no Internet Explorer. Para reduzir esse problema, altere as Configurações de rede do Java para a opção Conexão direta antes de instalar o agente.

Siga estas etapas:

1. Abra o Painel de controle Java no sistema do host em que você instala o agente.
2. Clique em Configurações de rede na guia Geral.

   A página Configurações de rede é exibida.
3. Selecione a opção Conexão direta e clique em OK para salvar as mudanças.
4. Instale o agente.

Instalação do CA Process Automation em ambientes de rede de pilha dupla (IPv4 e IPv6)

Se você instalar o CA Process Automation em ambientes de rede de pilha dupla (IPv4 e IPv6), a inicialização do CA Process Automation poderá falhar.

Sintoma:

Quando você instala o CA Process Automation em ambientes de rede de pilha dupla (IPv6 e IPv4), pode ter problemas ao abrir ou acessar os seguintes componentes do CA Process Automation na rede:

- Orquestradores de domínio
- Orquestradores
- Agentes

Solução:

Desative a pilha IPv6 no sistema do host no qual qualquer um dos seguintes componentes do CA Process Automation esteja em execução e reinicie os serviços:

- Orquestradores de domínio
- Orquestradores
- Agentes

Desempenho lento usando o MySQL

Sintoma:

Quando instalo o CA Process Automation usando o MySQL ou o Oracle como banco de dados, observo que o desempenho está insuficiente.

Solução:

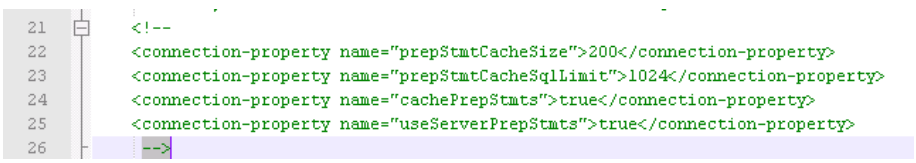
Pós-instalação, modificar o arquivo oasis-ds.xml para melhorar o desempenho do CA Process Automation.

Siga estas etapas:

1. Localizar e abrir o arquivo oasis-ds.xml, localizado em:

   install_dir/server/c2o/ext-deploy

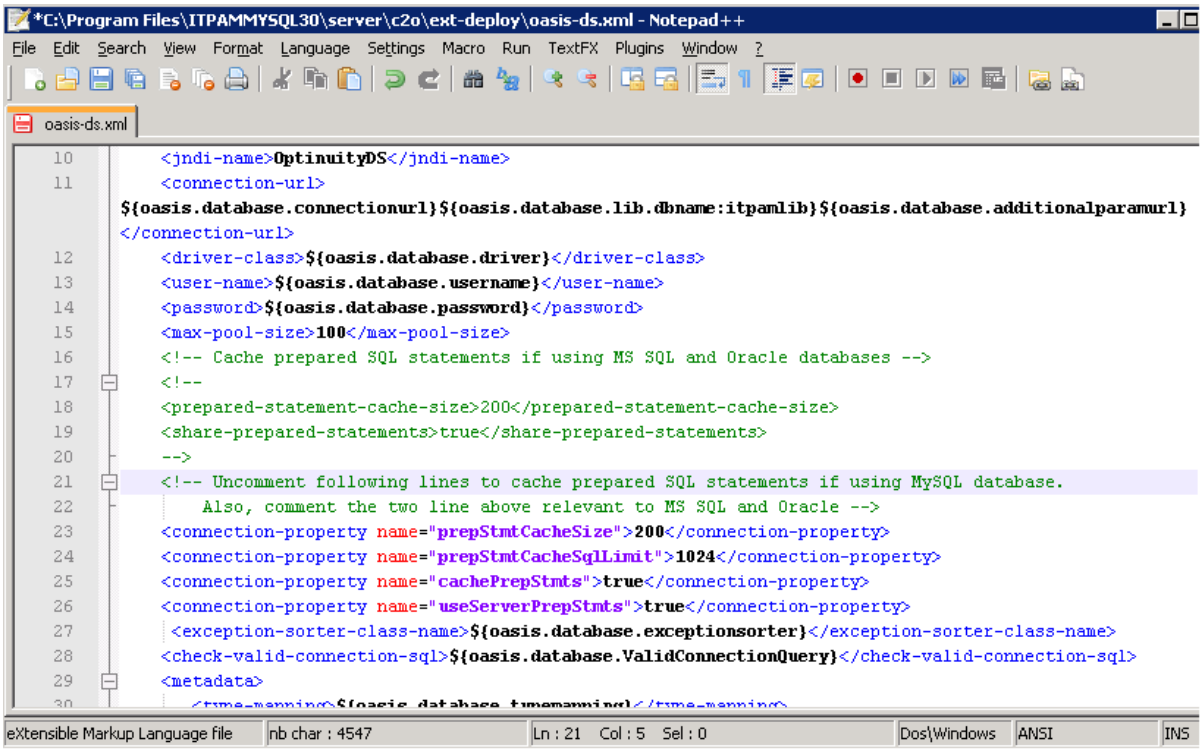
2. Não comentar as seguintes linhas:



3. Comentar as seguintes linhas:

```
16      <!-- Cache prepared SQL statements if using MS SQL and Oracle databases -->
17      <prepared-statement-cache-size>200</prepared-statement-cache-size>
18      <share-prepared-statements>true</share-prepared-statements>
```

O arquivo atualizado deve se parecer com este:



4. Reinicie o orquestrador.

Não é possível criar o banco de dados de tempo de execução

Sintoma:

Ao instalar um orquestrador e fornecer o banco de dados de tempo de execução na tela Banco de dados de tempo de execução, a seguinte exceção é acionada:

```
O banco de dados de tempo de execução está em uso por outro orquestrador.
```

Solução:

O CA Process Automation versão 4.0 não permite o compartilhamento de um mesmo banco de dados de tempo de execução entre orquestradores. Em geral, a solução para isso é criar o banco de dados de tempo de execução usando outro nome ou hospedá-lo em um servidor de banco de dados separado.

Use o procedimento a seguir **apenas** se você desejar manter as informações de tempo de execução desse banco de dados em uma nova instância do CA Process Automation. Esse raramente é o caso, e a redefinição de RuntimeDbOrchestratorID tem muitos efeitos colaterais indesejados, incluindo tornar impossível a conclusão da execução dos operadores nesse banco de dados de tempo de execução. Todos os agentes e os orquestradores secundários também devem ser reinstalados, entre outros problemas. Se você tiver qualquer dúvida se esse procedimento é apropriado para o seu problema, consulte o Suporte técnico antes de continuar.

Nessa versão, uma nova tabela Propriedades é criada no banco de dados com as seguintes colunas:

- PropKey
- PropValue

Sempre que um orquestrador usa um banco de dados de tempo de execução, uma nova linha é inserida na tabela Propriedades. A PropKey é RuntimeDbOrchestratorID e o PropValue é a ID exclusiva do orquestrador.

Quando outro orquestrador faz solicitações ao mesmo banco de dados, o banco de dados é validado na tabela Propriedades. Se a ID exclusiva do orquestrador solicitante não for semelhante ao Propvalue, a seguinte mensagem será exibida:

```
O banco de dados de tempo de execução está em uso por outro orquestrador.
```

Importante: as entradas do banco de dados de tempo de execução não são excluídas, mesmo depois que você desinstala o produto.

Para usar novamente o mesmo banco de dados para tempo de execução, execute a consulta SQL a seguir e exclua a linha correspondente da tabela Propriedades.

```
delete from properties where propkey = 'RuntimeDbOrchestratorID'
```

Não é possível executar os operadores Executar o script ou Executar programa no RHEL6

Sintoma:

Os operadores Executar o script ou Executar programa falham quando são executados no RHEL6.

Solução:

Os operadores Executar programa e Executar o script procuram por Korn shell (ksh) quando são executados em plataformas UNIX ou Linux. Por padrão, o RHEL 6 não possui o ksh instalado.

Esse problema pode ser resolvido por meio de uma destas opções:

- Instalando o ksh:

  O ksh pode ser instalado com o seguinte comando:

  ```
  yum install ksh
  ```

- Apontando um link simbólico para um shell válido

  Crie um link simbólico /bin/ksh e mapeie-o para qualquer shell (como Bash) existente no computador. Use este comando, em que /bin/bash é o local de bashshell:

  ```
  Em -s /bin/bash /bin/ksh
  ```

Apêndice E: Balanceador de carga do Apache

O balanceador de carga do Apache *não* oferece suporte à comunicação simplificada para agentes. Para utilizar a comunicação simplificada, você deverá usar o NGINX ou outro balanceador de carga com base em soquete da web. Se você usar o método de comunicação obsoleto, use essas instruções para instalar e configurar o balanceador de carga do Apache.

Consulte o tópico Sobre a comunicação do agente (na página 158) para obter mais informações.

Pré-requisitos do balanceador de carga do Apache

Um *orquestrador agrupado* é um conjunto de nós que são exibidos e que atuam como um único orquestrador, além de usar uma biblioteca compartilhada. Você pode agrupar qualquer orquestrador do CA Process Automation para obter alta disponibilidade, tolerância a falhas e escalabilidade.

Um balanceador de carga, como o servidor HTTP do Apache, é necessário para o agrupamento de qualquer orquestrador, incluindo o orquestrador de domínio. Um balanceador de carga não faz parte da instalação do CA Process Automation.

Embora o balanceador de carga possa ser configurado no mesmo host que um dos nós do orquestrador, é mais comum que ele resida em um host separado.

Um balanceador de carga é necessário *apenas* para um orquestrador em uma configuração agrupada e em configurações de SSO (Single Sign On - Logon único) específicas.

Importante: se um orquestrador for instalado sem antes instalar e configurar um balanceador de carga, você não poderá agrupar esse orquestrador posteriormente.

Configuração do balanceador de carga do Apache no Windows

Esta seção fornece instruções para instalar e configurar o balanceador de carga do Apache no Windows.

É possível configurar nos dois seguintes modos:

- Configuração básica (Windows) (na página 258)
- Configuração segura (Windows) (na página 262)

Configuração básica (Windows)

Esta seção fornece instruções para instalar e configurar o balanceador de carga do Apache no modo básico.

Observação: você pode usar um balanceador de carga diferente do Apache. No entanto, o orquestrador do CA Process Automation requer que algumas classes de solicitações sejam direcionadas para um nó específico no orquestrador agrupado. Portanto, o balanceamento de carga simples não é suficiente. Consulte a página Práticas recomendadas do CA Process Automation ou entre em contato com o suporte da CA para obter ajuda com as alternativas. A biblioteca inclui links para essas páginas.

Siga estas etapas:

1. Instale um balanceador de carga e prepare modelos de configuração (Windows) (na página 258).
2. Configurar a comunicação básica (na página 260).
3. (Opcional) Configure o balanceador de carga Apache para Catalyst RESTful API (Windows) (na página 261)

   Observação: para que um servidor web do Apache possa encaminhar solicitações https para operadores do Catalyst, os certificados SSL devem estar no formato PEM. Se necessário, Gere arquivos de certificado SSL (na página 50).

Instale um balanceador de carga e prepare modelos de configuração (Windows)

A mídia de instalação do CA Process Automation inclui o seguinte arquivo de configuração de exemplo do balanceador de carga Apache que você pode usar como ponto de partida para a configuração:

```
ApacheConfig.zip
```

As instruções a seguir pressupõem que o balanceador de carga do Apache 2.2 já esteja dedicado ao CA Process Automation. Primeiro, instale um balanceador de carga do Apache. Em seguida, extraia os arquivos do arquivo zip ApacheConfTemplates do CA Process Automation na pasta Conf sob a pasta de Instalação do Apache.

Siga estas etapas:

1. Efetue logon no host em que o balanceador de carga deverá ser executado.

   O balanceador de carga geralmente não está no mesmo host que o orquestrador de domínio. No entanto, o host com o orquestrador de domínio deve ser roteável a partir do balanceador de carga.

2. Baixe e instale o balanceador de carga do Apache mais recente com suporte SSL. Siga as instruções do fornecedor.

3. Faça download do arquivo a seguir para a versão instalada do Apache:

   `mod_jk.so`

   É recomendável que você faça download da versão mais recente.

4. Copie o arquivo mod_jk.so na seguinte pasta:

   `apache_install_dir``\modules`

5. Navegue até a seguinte pasta na mídia de instalação do CA Process Automation:

   `install_dir``\DVD1\ApacheConfTemplates`

6. Extrair os seguintes arquivos do ApacheConfig.zip:

   `mod-jk.conf`

   `httpd-proxy.conf`

   `uriworkermap.properties`

   `workers.properties`

   `httpd VIRTUALHOST_EXAMPLE FILE`

   Observação: o arquivo httpd VIRTUALHOST_EXAMPLE extraído contém texto que você pode recortar e colar no arquivo httpd do Apache ao configurar as comunicações seguras. O texto necessário também está na documentação.

7. Copie os seguintes arquivos extraídos da pasta *apache_install_dir*\conf:

   `mod-jk.conf`

   `httpd-proxy.conf`

   `uriworkermap.properties`

   `workers.properties`

   Observação: se você não tiver um balanceador de carga do Apache 2.2 para dedicar, mescle as informações de configuração das propriedades de modelo de exemplo e dos arquivos Conf com seus arquivos existentes. Como precaução, faça backup de seus arquivos antes de modificá-los.

Configurar a comunicação básica

Você pode configurar um balanceador de carga para a comunicação básica com os nós do orquestrador de domínio ou outro orquestrador.

Siga estas etapas:

1. Vá até a seguinte pasta:

   apache_install_dir\conf

   Esta pasta contém worker.properties e mod-jk.conf.

2. Abra o arquivo workers.properties.
3. Adicione o primeiro nó definindo node1 que começa com a seguinte linha:
   `worker.`**`node1`**`.host=<Digite o nome do host do node1 aqui>`
4. Nessa linha, substitua o espaço reservado *Enter node1 hostname here* para worker.node1.host pelo valor válido.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.

5. Salve e feche o arquivo worker.properties.
6. Abra o arquivo mod-jk.conf.
7. Não comentar a seguinte linha:

   ```
   # JkMountFile conf/uriworkermap.properties
   ```

8. Salve e feche o arquivo mod-jk.conf.
9. Abra o arquivo httpd.conf.
10. Adicione a seguinte entrada ao final do arquivo httpd.conf:
    ```
    Módulo de balanceamento de carga n°
    Incluir conf/mod-jk.conf
    ```
11. Salve e feche o arquivo httpd.conf.

Configure o balanceador de carga Apache para Catalyst RESTful API (Windows)

É possível configurar o servidor web do Apache (balanceador de carga) para a API RESTful do Catalyst. As alterações na configuração do Apache se baseiam no seu balanceador de carga já configurado para o CA Process Automation.

Depois de configurar o CA Process Automation em um modo de agrupamento, execute as tarefas de pós-instalação.

Siga estas etapas:

1. Vá até a seguinte pasta na mídia de instalação do CA Process Automation:

   install_dir\DVD1\ApacheConfTemplates

2. Extrair os seguintes arquivos do ApacheConfig.zip:

   `httpd-proxy.conf`

3. Copie o arquivo httpd-proxy.conf para o diretório *apacheHome*/conf/extra.

4. Atualize as linhas a seguir nos hosts virtuais http e https para substituir os nomes de host do orquestrador para BalancerMember.

   Integrantes do nó UnSecured

   ```
   <Balanceador do proxy://ucfcluster>
   BalancerMember  http://< Enter node1 hostname>:7000
   BalancerMember  http://< Enter node2 hostname>:7000
   ```

   Integrantes do nó protegidos

   ```
   <Balanceador do proxy://sslcluster>
   BalancerMember  https://< Enter node1 hostname>:7443
   BalancerMember  https://< Enter node2 hostname>:7443
   ```

5. Substitua o espaço reservado <Inserir nome do host do node*x*> por worker.node*x*.host com o valor válido.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.

6. Salve o arquivo httpd-proxy.conf.

7. Abra o arquivo *apacheHome*/conf/httpd.conf e verifique se as portas 7000 e 7443 não são usadas.

8. Adicione a seguinte linha ao final do arquivo httpd.conf:

   `Include conf/extra/httpd-proxy.conf`

9. Siga o procedimento em Gerar arquivos de certificado SSL (na página 50) para gerar os arquivos c2okey2.pem e c2ocert.pem.

10. Copie os arquivos gerados para o diretório *apacheHome/*conf.

11. Salve os arquivos modificados e reinicie o servidor web do Apache.

Configuração segura (Windows)

Esta seção fornece instruções para instalar e configurar o balanceador de carga do Apache no modo seguro.

Siga estas etapas:

1. Instalar um balanceador de carga e preparar modelos de configuração (na página 258).
2. Gerar arquivos de certificado SSL (na página 50)

   Observação: para que um servidor web do Apache possa encaminhar solicitações https para operadores do Catalyst, os certificados SSL devem estar no formato PEM.
3. Configure a comunicação segura (Windows) (na página 264).
4. Configure o balanceador de carga Apache para Catalyst RESTful API (Windows) (na página 261)

Gerar arquivos de certificado SSL

A geração dos certificados SSL deve ser feita *depois* de instalar o CA Process Automation, mas *antes* de configurar a comunicação segura para o balanceador de carga. Os certificados SSL não são necessários se você deseja usar a comunicação básica, não segura, no balanceador de carga.

Uma vez gerado, o local do arquivo de certificado deve ser identificado quando você definir a configuração do balanceador de carga para a comunicação segura.

Siga estas etapas:

1. Faça download e instale o OpenSSL de um fornecedor.

   Observação: certifique-se de que o host no qual você instala o OpenSSL possui o JDK instalado.

2. Depois de instalar o CA Process Automation em modo de agrupamento (e pelo menos um nó estiver instalado), o assistente de instalação do CA Process Automation irá gerar o arquivo c2okeystore no seguinte local:

   `\server_location\c2o\.config`

   Copie o c2okeystore e cole-o no seguinte diretório:

   `\jdk_location\bin`

   É possível executar os comandos localmente a partir desse local.

3. Use o keytool no JDK para importar o armazenamento de chaves para o formato pksc12, como segue:

   a. Vá para o diretório jdk_location\bin e execute o seguinte comando:

      ```
      keytool -importkeystore -srckeystore c2okeystore
      -srcstoretype jks -destkeystore c2okeystore.p12
      -deststoretype pkcs12
      ```

      O console solicita a senha do armazenamento de chaves de destino.

      Observação: o arquivo OasisConfig.properties contém a senha do armazenamento de chaves. Localize o arquivo nesse diretório: `\server_location\c2o\.config\`

      Abra o arquivo e copie a senha. O valor pode ser encontrado próximo à entrada KEYSTOREID=.

      Por exemplo, KEYSTOREID=723e1830-a98c-49a1-8f16-a0794c872835. A senha é 723e1830-a98c-49a1-8f16-a0794c872835.

   b. Cole a senha no prompt de senha do armazenamento de chaves no console aberto.

   c. Quando solicitado, digite novamente a senha.

   d. No prompt de senha da chave de origem, digite a senha novamente.

      Um arquivo c2okeystore.p12 é gerado no diretório \jdk_location\bin.

   e. É necessário converter o armazenamento de chaves p12 formatado em arquivos de chave e de certificado PEM formatados. Para fazê-lo, execute o comando openssl no local do diretório \jdk_location\bin:

      ```
      openssl pkcs12 -nocerts -in c2okeystore.p12 -out c2okey.pem
      ```

   f. No prompt da senha de importação, digite a senha do armazenamento de chaves.

   g. No prompt da frase secreta do PEM, digite qualquer frase.

h. Digite novamente a frase secreta do PEM.

i. Execute o comando a seguir no local do diretório \jdk_location\bin:
```
openssl pkcs12 -clcerts -in c2okeystore.p12 -out c2ocert.pem
```

j. No prompt da senha de importação, digite a senha do armazenamento de chaves.

k. No prompt da frase secreta do PEM, digite a frase que você criou anteriormente para a etapa g.

l. Digite novamente a frase secreta do PEM.

m. Execute o comando a seguir no local do diretório \jdk_location\bin:
```
openssl rsa -in c2okey.pem -out c2okey2,pem
```

n. No prompt da frase secreta do PEM, digite a frase que você criou anteriormente para a etapa g.

o. Digite novamente a frase secreta do PEM.

p. Copie os arquivos c2okey2.pem e c2ocert.pem para o diretório \conf do balanceador de carga.

Observação: faça backup desses arquivos.

Configure a comunicação segura (Windows)

Você pode configurar um balanceador de carga para a comunicação segura. Nas etapas a seguir, *certloc* indica o local do certificado.

Siga estas etapas:

1. Instalar um balanceador de carga e preparar modelos de configuração (na página 258).
2. Abra o arquivo workers.properties.
3. Adicione o primeiro nó definindo node1 que começa com a seguinte linha:
```
worker.node1.host=<adicione o nome de host do node1 aqui>
```
4. Nessa linha, substitua o espaço reservado *Enter node1 hostname here* para worker.node1.host pelo valor válido.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.
5. Salve e feche a arquivo workers.

6. Revise os locais padrão de CA no arquivo openssl no diretório a seguir.

   apache_install_location/conf

7. Crie ou obtenha um arquivo de certificado e um arquivo de chave privada com um "Nome comum" que corresponda a "ServerName" em httpd.conf.

   Por exemplo, as etapas a seguir mostram como usar o utilitário openssl que é fornecido com o balanceador de carga Apache para criar um arquivo de certificado. Opções adicionais controlam a expiração do certificado, os nomes de arquivos e os algoritmos. Se o seu site possui requisitos especiais, consulte a documentação oferecida pelo fornecedor.

   a. Abra um prompt de comando.

   b. Altere os diretórios para a pasta bin do Apache.

      cd *apache_install_location*/bin

   c. Crie um arquivo de Solicitação de assinatura de certificado (CSR) e arquivos PEM. Para isso, digite o seguinte comando, em que "mypamserver" é um nome de sua escolha:

      openssl req -config ../conf/openssl.cnf -new -out *mypamserver*.csr

      Você será solicitado a inserir a senha do arquivo PEM e outras informações de identificação.

      - Pode aceitar os valores padrão para a maioria das informações de identificação (por exemplo, nome do país, nome do estado ou província, nome da localidade, nome da empresa e nome da unidade organizacional). Para deixar um campo em branco, insira um ponto (.).
      - Quando o prompt Nome comum for exibido, digite a parte do nome do host de "ServerName" como o valor em *apache_install_location/*conf/httpd.conf.

        Por exemplo, se ServerName em httpd.conf possuir o valor myhost.mycompany.com:80, especifique **myhost.mycompany.com** como o Nome comum.
      - Os seguintes campos são opcionais: endereço de email, dir, uma senha desafiadora e um nome de empresa opcional.

      O balanceador de carga Apache cria *mypamserver*.csr e *privkey*.pem no diretório atual.

   d. Crie sua chave RSA privada. Para isso, digite uma passphrase para *privkey*.pem quando o balanceador de carga Apache solicitar.

      openssl rsa -in *privkey*.pem -out *mypamserver*.key

   e. Crie seu certificado.

      openssl x509 -in *mypamserver*.csr -out *mypamserver*.cert -req -signkey *mypamserver*.key

8. Feche o prompt de comando e abra o Windows Explorer para copiar e excluir os arquivos gerados:
   a. Selecione ou crie a pasta *certloc* para manter seu certificado e os arquivos de chave privada.
   b. Abra a pasta *apache_install_dir*\bin no local em que os arquivos CERT e KEY foram gerados.
   c. Arraste e solte (ou seja, mova) *mypamserver*.cert e *mypamserver*.key para *certloc*.
   d. Exclua os arquivos intermediários criados na pasta *apache_install_dir/*bin. Os arquivos intermediários incluem *mypamserver*.CSR, *privkey*.PEM e .RND.
9. Faça backup dos arquivos que você criou.
10. Use um editor de texto para modificar o arquivo de texto httpd (*apache_install_location*\conf\httpd.conf) da seguinte maneira:
    a. Não comentar as seguintes linhas:

```
LoadModule rewrite_module modules/mod_rewrite.so

LoadModule ssl_module modulws/mod_ssl.so

Incluir conf/extra/httpd-ssl.conf
```

    b. Adicione as linhas a seguir no final de httpd.conf. É possível copiar e colar o texto do arquivo httpd VIRTUALHOST_EXAMPLE extraído do SecureDomainConfig_ Template.zip.

```
<VirtualHost *:80>
JkMountFile conf/uriworkermap.properties
RewriteEngine ativo
RewriteCond %{HTTPS} inativo
RewriteCond http://%{HTTP_HOST}%{REQUEST_URI}
!^http://.*c2orepository*|MirroringRequestProcessor*|mirror
ingrepository*|StartAgent*|genericNoSecurity*|soapAttachmen
t*
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
Nº do módulo de balanceamento de carga
include conf/mod-jk.conf
```

    c. Salve o arquivo httpd.conf modificado e feche o editor.
11. Faça backup dos arquivos que você editou.

12. Use um editor de texto para modificar o arquivo de configuração *apache_install_location/*conf/extra/httpd-ssl da seguinte maneira:
    a. Remova o comentário (se estiver comentado) do seguinte texto: "Listen 443"
    b. Altere o local SSLCertificateFile para .../*certloc/mypamserver.*cert.

       ```
       SSLCertificateFile "C:/certloc/mypamserver.cert"
       ```

    c. Altere o local SSLCertificateKeyFile para .../*certloc/mypamserver.*key.

       ```
       SSLCertificateKeyFile "C:/certloc/mypamserver.key"
       ```

    d. Adicione as seguintes linhas ao final do elemento <VirtualHost>, antes do elemento </VirtualHost>:

       ```
       SSLOptions +StdEnvVars +ExportCertData
       JkMountFile conf/uriworkermap.properties
       ```

    e. Salve o arquivo httpd.conf-ssl modificado e feche o editor.
13. Reinicie o serviço do Apache. Para fazer isso, clique em Programas, Apache HTTP Server 2.2, Servidor Control Apache, Reiniciar no menu Iniciar.

    As mudanças entram em vigor.

Configuração do balanceador de carga do Apache não no Windows

Esta seção fornece instruções para instalar e configurar o balanceador de carga do Apache não no Windows.

É possível configurar nos dois seguintes modos:

- Configuração básica (não no Windows) (na página 268)
- Conexão Segura (não no Windows) (na página 272)

Configuração básica (não no Windows)

Esta seção fornece instruções para instalar e configurar o balanceador de carga do Apache no modo básico.

Observação: você pode usar um balanceador de carga diferente do Apache. No entanto, o orquestrador do CA Process Automation requer que algumas classes de solicitações sejam direcionadas para um nó específico no orquestrador agrupado. Portanto, o balanceamento de carga simples não é suficiente. Consulte a página Práticas recomendadas do CA Process Automation ou entre em contato com o suporte da CA para obter ajuda com as alternativas. A biblioteca inclui links para essas páginas.

Siga estas etapas:

1. Instale um balanceador de carga e prepare os modelos de configuração (não no Windows) (na página 268).
2. Configurar a comunicação básica (na página 260).
3. Configure o balanceador de carga Apache para Catalyst RESTful API (não no Windows) (na página 270)

   Observação: para que um servidor web do Apache possa encaminhar solicitações https para operadores do Catalyst, os certificados SSL devem estar no formato PEM. Se necessário, Gere arquivos de certificado SSL (na página 50).

Instale um balanceador de carga e prepare os modelos de configuração (não no Windows)

A mídia de instalação do CA Process Automation inclui o seguinte arquivo de configuração de exemplo do balanceador de carga Apache que você pode usar como ponto de partida para a configuração:

```
ApacheConfig.zip
```

As instruções a seguir pressupõem que o balanceador de carga do Apache 2.2 seja dedicado ao CA Process Automation. Primeiro, instale um balanceador de carga do Apache. Em seguida, extraia os arquivos do arquivo zip ApacheConfTemplates do CA Process Automation na pasta Conf sob a pasta de Instalação do Apache.

Siga estas etapas:

1. Efetue logon no host em que o balanceador de carga deverá ser executado.

   O balanceador de carga geralmente não está no mesmo host que o orquestrador de domínio. No entanto, o host com o orquestrador de domínio deve ser roteável a partir do balanceador de carga.

2. Baixe e instale o balanceador de carga do Apache mais recente. Por exemplo, navegue até a pasta extraída e execute os seguintes comandos:

   ```
   ./configure -prefix=<install location>-enable-so -enable-mods-shared=all
   -enable-mod-rewrite --with-z=<zlib home>--with-included-apr  --with-mpm=worker
   --enable-ssl --with-ssl=<ssl home>
   ```

   ```
   Make
   ```

   ```
   Make install
   ```

3. Fazer download e instalar o conector Tomcat para criar o módulo mod_jk. Por exemplo, navegue até o *<local extraído do conector Tomcat>/*native/ e execute os seguintes comandos:

   ```
   ./configure --with-apxs=<install location>/bin/apxs
   make
   make install
   ```

4. Verifique se o servidor Apache está ativo e em execução.

5. Vá até a seguinte pasta na mídia de instalação do CA Process Automation:

   install_dir\DVD1\ApacheConfTemplates

6. Extrair os seguintes arquivos do ApacheConfig.zip:

   ```
   mod-jk.conf
   ```

   ```
   httpd-proxy.conf
   uriworkermap.properties
   workers.properties
   httpd VIRTUALHOST_EXAMPLE FILE
   ```

   Observação: o arquivo httpd extraído contém texto que você pode recortar e colar no arquivo httpd do Apache ao configurar as comunicações seguras. O texto necessário também está na documentação.

7. Copie os arquivos extraídos na seguinte pasta:

   apache_install_dir\conf

Configure o balanceador de carga Apache para Catalyst RESTful API (não no Windows)

É possível configurar o servidor web do Apache (balanceador de carga) para a API RESTful do Catalyst. Faça as alterações na configuração do Apache no balanceador de carga já configurado para o CA Process Automation.

Verifique se os seguintes arquivos binários estão instalados no servidor Apache.

```
mod_proxy.so
mod_proxy_balancer.so
mod_proxy_http.so
```

Siga estas etapas:

1. Vá até a seguinte pasta na mídia de instalação do CA Process Automation:

   install_dir\DVD1\ApacheConfTemplates

2. Extraia os seguintes arquivos do ApacheConfig.zip:

   `httpd-proxy.conf`

3. Copie httpd-proxy.conf para o seguinte diretório:

   `apacheHome/conf/extra`

4. Abra httpd-proxy.conf e comentar as seguintes linhas:

   ```
   LoadModule proxy_module modules/mod_proxy.so

   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so

   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

5. Navegue de volta para a pasta *apache_install_dir*\conf, abra httpd.conf e remova os comentários das seguintes linhas (se houver comentários):

   ```
   LoadModule proxy_module modules/mod_proxy.so

   LoadModule proxy_balancer_module modules/mod_proxy_balancer.so

   LoadModule proxy_http_module modules/mod_proxy_http.so
   ```

6. Atualize as linhas a seguir nos hosts virtuais http e https para substituir os nomes de host do orquestrador para BalancerMember.

   Integrantes do nó UnSecured

   - Node 1

     `BalancerMember  http://< Enter node1 hostname>:7000`

   - Node 2

     `BalancerMember  http://< Enter node2 hostname>:7000`

   Integrantes do nó protegidos

- Node 1

  ```
  BalancerMember  https://< Enter node1 hostname>:7443
  ```

- Node 2

  ```
  BalancerMember  https://< Enter node2 hostname>:7443
  ```

7. Substitua o espaço reservado “Enter node1 hostname here" para worker.node1.host pelo valor real.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.

8. Salve o arquivo httpd-proxy.conf.
9. Abra o arquivo apacheHome/conf/httpd.conf e verifique se as portas 7000 e 7443 não são usadas.
10. Adicione a seguinte linha ao final do arquivo httpd.conf:

    ```
    Include conf/extra/httpd-proxy.conf
    ```

11. Gerar arquivos de certificado SSL (na página 50) para gerar os arquivos c2okey2.pem e c2ocert.pem.
12. Copie os arquivos gerados para o diretório *apacheHome/*conf.
13. Reinicie o servidor web Apache.

Configurar configuração segura (não no Windows)

Esta seção fornece instruções para instalar e configurar o balanceador de carga do Apache no modo seguro.

Observação: você pode usar um balanceador de carga diferente do Apache. No entanto, o orquestrador do CA Process Automation requer que algumas classes de solicitações sejam direcionadas para um nó específico no orquestrador agrupado. Portanto, o balanceamento de carga simples não é suficiente. Consulte a página Práticas recomendadas do CA Process Automation ou entre em contato com o suporte da CA para obter ajuda com as alternativas. A biblioteca inclui links para essas páginas.

Siga estas etapas:

1. Instale um balanceador de carga e prepare os modelos de configuração (não no Windows) (na página 268).
2. Configure a configuração segura (não no Windows) (na página 272).
3. Configure o balanceador de carga Apache para Catalyst RESTful API (não no Windows) (na página 270)

   Observação: para que um servidor web do Apache possa encaminhar solicitações https para operadores do Catalyst, os certificados SSL devem estar no formato PEM. Se necessário, gere novamente os arquivos de certificado SSL (na página 50).

Configurar configuração segura (não no Windows)

Você pode configurar um balanceador de carga para a comunicação segura. Nas etapas a seguir, *certloc* indica o local do certificado.

Siga estas etapas:

1. Instalar um balanceador de carga e preparar modelos de configuração (na página 258).
2. Abra o arquivo workers.properties.
3. Adicione o primeiro nó definindo node1 que começa com a seguinte linha:

   ```
   worker.node1.host=<adicione o nome de host do node1 aqui>
   ```

4. Nessa linha, substitua o espaço reservado *Enter node1 hostname here* para worker.node1.host pelo valor válido.

   Observação: os valores válidos são o endereço IP, o FQDN ou o alias de DNS que é resolvido para o host em que você está instalando o nó inicial do orquestrador de domínio. O valor válido é o mesmo usado para “Server Host” ao instalar o orquestrador de domínio.

5. Salve e feche a arquivo workers.

6. Revise os locais padrão de CA no arquivo openssl no diretório a seguir.

   apache_install_location/conf

7. Crie ou obtenha um arquivo de certificado e um arquivo de chave privada com um "Nome comum" que corresponda a "ServerName" em httpd.conf.

   Por exemplo, as etapas a seguir mostram como usar o utilitário openssl que é fornecido com o balanceador de carga Apache para criar um arquivo de certificado. Opções adicionais controlam a expiração do certificado, os nomes de arquivos e os algoritmos. Se o seu site possui requisitos especiais, consulte a documentação oferecida pelo fornecedor.

   a. Abra um prompt de comando.

   b. Altere os diretórios para a pasta bin do Apache.

      cd *apache_install_location*/bin

   c. Crie um arquivo de Solicitação de assinatura de certificado (CSR) e arquivos PEM. Para isso, digite o seguinte comando, em que "mypamserver" é um nome de sua escolha:

      openssl req -new -out mypamserver.csr

      Você será solicitado a inserir a senha do arquivo PEM e outras informações de identificação.

      - Pode aceitar os valores padrão para a maioria das informações de identificação (por exemplo, nome do país, nome do estado ou província, nome da localidade, nome da empresa e nome da unidade organizacional). Para deixar um campo em branco, insira um ponto (.).
      - Quando o prompt Nome comum for exibido, digite a parte do nome do host de "ServerName" como o valor em *apache_install_location/*conf/httpd.conf.

        Por exemplo, se ServerName em httpd.conf possuir o valor myhost.mycompany.com:80, especifique **myhost.mycompany.com** como o Nome comum.

      - Os seguintes campos são opcionais: endereço de email, dir, uma senha desafiadora e um nome de empresa opcional.

      O balanceador de carga Apache cria *mypamserver*.csr e *privkey*.pem no diretório atual.

   d. Crie sua chave RSA privada. Para isso, digite uma passphrase para *privkey*.pem quando o balanceador de carga Apache solicitar.

      openssl rsa -in *privkey*.pem -out *mypamserver*.key

   e. Crie seu certificado.

      openssl x509 -in *mypamserver*.csr -out *mypamserver*.cert -req -signkey *mypamserver*.key

8. Feche o prompt de comando e abra o Windows Explorer para copiar e excluir os arquivos gerados:
   a. Selecione ou crie a pasta *certloc* para manter seu certificado e os arquivos de chave privada.
   b. Abra a pasta *apache_install_dir*\bin no local em que os arquivos CERT e KEY foram gerados.
   c. Arraste e solte (ou seja, mova) *mypamserver*.cert e *mypamserver*.key para *certloc*.
   d. Exclua os arquivos intermediários criados na pasta *apache_install_dir/*bin. Os arquivos intermediários incluem *mypamserver*.CSR, *privkey*.PEM e .RND.
9. Faça backup dos arquivos que você criou.
10. Use um editor de texto para modificar o arquivo de texto httpd (*apache_install_location*\conf\httpd.conf) da seguinte maneira:
    a. Não comentar as seguintes linhas:

       ```
       LoadModule rewrite_module modules/mod_rewrite.so

       LoadModule ssl_module modulws/mod_ssl.so

       Incluir conf/extra/httpd-ssl.conf
       ```

    b. Adicione as linhas a seguir no final de httpd.conf. É possível copiar e colar o texto do arquivo httpd VIRTUALHOST_EXAMPLE extraído do SecureDomainConfig_ Template.zip.

       ```
       <VirtualHost *:80>
       JkMountFile conf/uriworkermap.properties
       RewriteEngine ativo
       RewriteCond %{HTTPS} inativo
       RewriteCond http://%{HTTP_HOST}%{REQUEST_URI}
       !^http://.*c2orepository*|MirroringRequestProcessor*|mirror
       ingrepository*|StartAgent*|genericNoSecurity*|soapAttachmen
       t*
       RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
       </VirtualHost>
       Nº do módulo de balanceamento de carga
       include conf/mod-jk.conf
       ```

    c. Salve o arquivo httpd.conf modificado e feche o editor.
11. Faça backup dos arquivos que você editou.

12. Use um editor de texto para modificar o arquivo de configuração *apache_install_location/*conf/extra/httpd-ssl da seguinte maneira:
    a. Remova o comentário (se estiver comentado) do seguinte texto: "Listen 443"
    b. Altere o local SSLCertificateFile para .../*certloc/mypamserver.*cert.

       ```
       SSLCertificateFile "/usr/local/certloc/mypamserver.cert"
       ```

    c. Altere o local SSLCertificateKeyFile para .../*certloc/mypamserver.*key.

       ```
       SSLCertificateKeyFile "/usr/local/certloc/mypamserver.key"
       ```

    d. Adicione as seguintes linhas ao final do elemento <VirtualHost>, antes do elemento </VirtualHost>:

       ```
       SSLOptions +StdEnvVars +ExportCertData
       JkMountFile conf/uriworkermap.properties
       ```

    e. Salve o arquivo httpd.conf-ssl modificado e feche o editor.
13. Reinicie o serviço do Apache. Para fazer isso, clique em Programas, Apache HTTP Server 2.2, Servidor Control Apache, Reiniciar no menu Iniciar.

    As mudanças entram em vigor.

Apêndice F: Exemplos de atualização

Esta seção contém os seguintes tópicos:

Exemplo: atualizar qualquer nó do orquestrador de domínio da Release 3.1 SP01 para a 4.2 no Windows

O exemplo a seguir é o primeiro de dois exemplos relacionados sobre a atualização de um orquestrador de domínio agrupado da Release 3.1 SP01 para a 4.2 em um sistema operacional Windows. Os exemplos incluem instantâneos selecionados e comentários do seguinte cenário:

- Nó 1 do orquestrador de domínio - pam-sandbox-n1
- Nó 2 do orquestrador de domínio - pam-sandbox-n2
- Balanceador de carga do orquestrador de domínio - pam-sandbox-LB

Estas são as etapas:

1. Efetue logon no host com o nó do orquestrador de domínio agrupado que você planeja atualizar.
2. Abra a release do CA Process Automation que está sendo atualizada. Por exemplo, no menu Iniciar, selecione Programas, CA, Domínio do CA Process Automation 3.1 SP1, Iniciar o CA Process Automation.

   Observação: essa é uma maneira fácil de verificar se o CA EEM está em execução e se o servidor de banco de dados está ativo. Isto é um pré-requisito para a atualização.

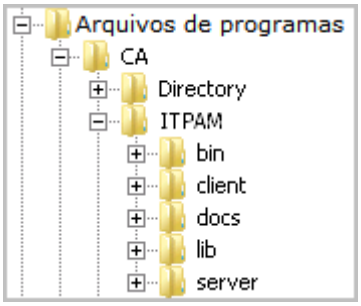
3. Clique em Sair, feche o console de gerenciamento do CA Process Automation e interrompa o serviço do orquestrador. (Se você abrir Serviços, é possível verificar se o serviço não está com o status Iniciado.) Não prossiga enquanto o status for "Interrompendo". Atualize essa exibição e aguarde até que o campo Status esteja limpo.

4. Vá até a pasta DVD1 da mídia de instalação e inicie o Domain_Installer_windows.bat.

5. Clique em Avançar para percorrer as páginas iniciais do assistente de instalação do instalador de terceiros:

   - Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation
   - Contrato de licença - Eu aceito os termos do Contrato de Licença

6. Para a opção Selecione o diretório de destino, navegue até o diretório exato que contém os arquivos do CA Process Automation 3.1sp01: bin, cliente, documentos, lib e servidor. Esse diretório pode ter o nome padrão ou um nome fornecido anteriormente.



Importante: Você deve apontar para o diretório correto para que o processo de instalação reconheça as suas opções de configuração anteriores.

7. Clique em Avançar para percorrer os pré-requisitos para instalação do CA Process Automation.

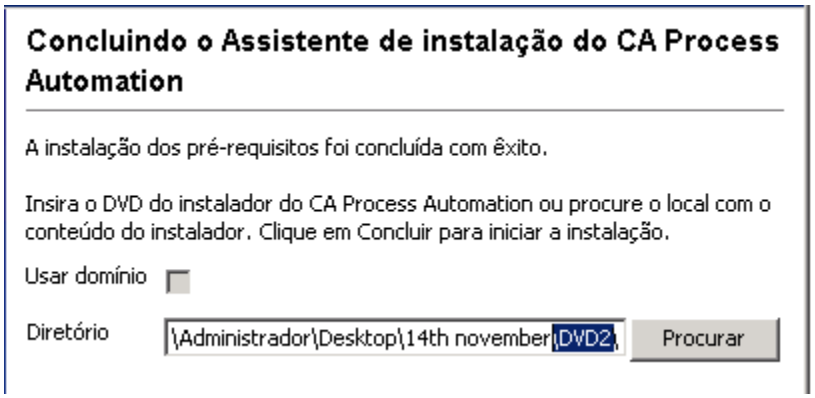
   A instalação de componentes de terceiros é iniciada.

8. Quando o JDBC Jars da página de instalação é exibido, clique em Adicionar arquivos, se estiver usando um servidor de banco de dados do MySQL ou um SQL Server. Vá até o local do arquivo jar apropriado.

   Por exemplo, o driver do JDBC para o SQL Server foi alterado, procure DVD1\drivers\jtds-1.3.jar para o SQL Server.

9. Quando Concluindo o Assistente de instalação do CA Process Automation é exibido,

   a. Altere o último diretório do caminho exibido de DVD1 para DVD2.



   b. Clique em Concluir.

      A seguinte mensagem será exibida: "Copiando o instalador do CA Process Automation. Isso pode levar alguns minutos. Aguarde."

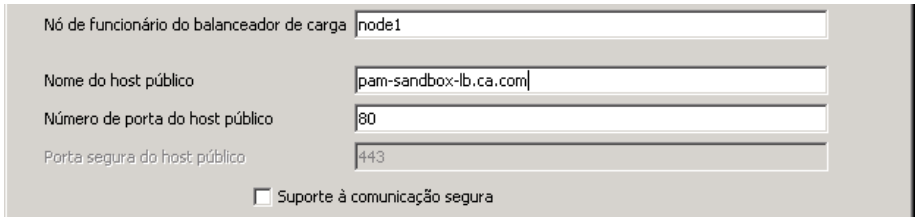
10. Quando Bem-vindo ao Assistente de instalação de domínio do CA Process Automation é exibido, clique nas páginas iniciais do assistente:

    - Idioma
    - Bem-vindo ao Assistente de instalação de domínio do CA Process Automation
    - Contrato de Licença - Eu aceito os termos do Contrato de Licença.
    - Diretório inicial do Java - este é selecionado automaticamente, por exemplo, C:\Arquivos de Programas\Java\jdk1.7.0_x.
    - Reinstalar/configurar - a opção Reinstalar significa **Atualização**.

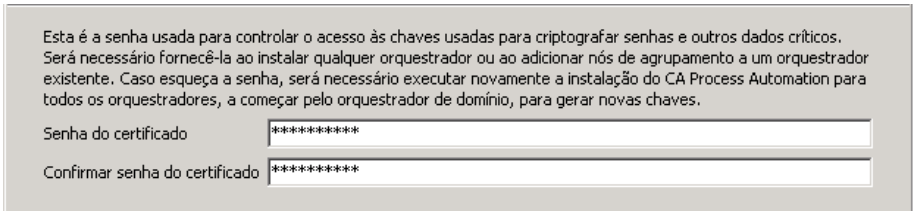
      A mensagem de cópia da configuração é exibida.

    - Tela de configuração

      O exemplo a seguir inclui os dados de exemplo:

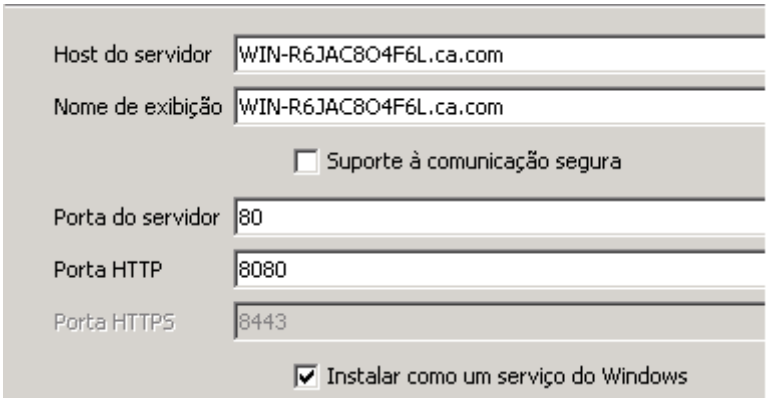


11. Quando Definir senha do certificado é exibido, insira a *mesma* senha do certificado que foi usada na release anterior e, em seguida, clique em Avançar.

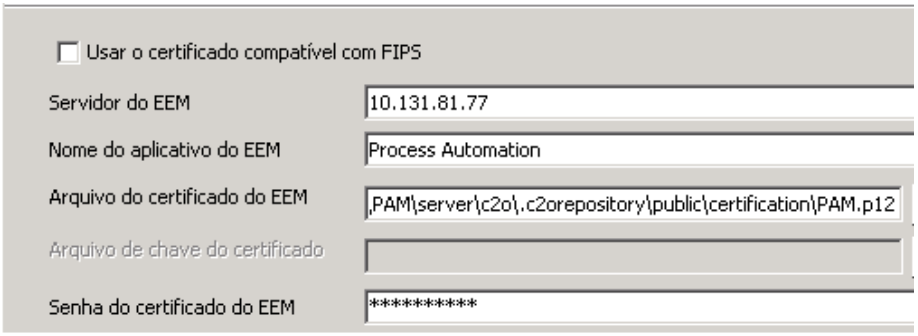


12. Clique em Avançar para selecionar a pasta do menu Iniciar - o padrão é CA Process Automation 4.2
13. Para obter as Propriedades gerais, clique em Avançar. Instalar como um serviço do Windows é selecionado por padrão.

    O exemplo a seguir inclui os dados de exemplo:

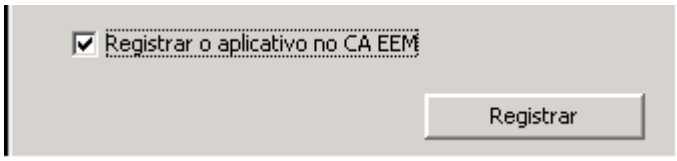


14. Clique em Avançar para proceder para as seguintes páginas:
    - Diretório temporário de scripts
    - Diretiva de execução do PowerShell
15. Quando Configurações de Segurança do EEM (Embedded Entitlements Manager) é exibido, as entradas da configuração anterior são preenchidas por padrão. Por exemplo:

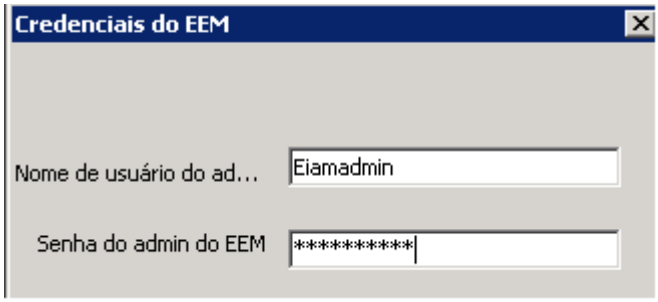


a. Ignore o campo Domínio padrão do Active Directory, a menos que tenha configurado o CA EEM para usar vários Microsoft Active Directories. Nesse caso, digite o nome de um dos AD que você configurou.

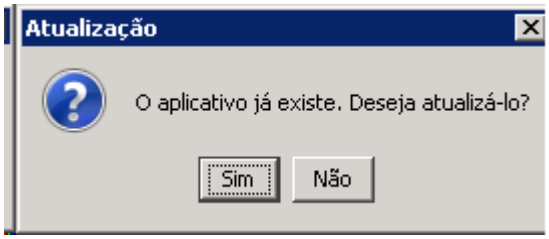
b. Selecione Registrar o aplicativo com o CA EEM e clique em Registrar.



c. Forneça credenciais para efetuar logon no CA EEM como o administrador EiamAdmin e clique em OK.



d. Clique em Sim para concordar com a atualização.

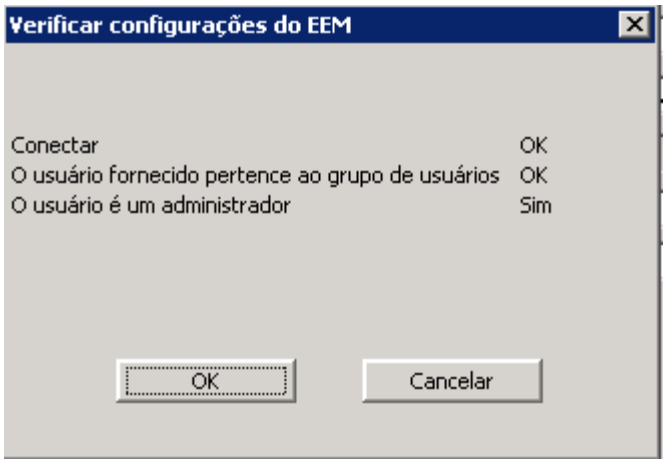


e. Clique em OK na mensagem "Aplicativo atualizado".

f. (Opcional). Clique em Testar configurações do EEM e conclua Verificar configurações do EEM:

- Se as credenciais de usuário estiverem armazenadas no CA EEM, digite o nome de usuário e a senha da sua conta de usuário do CA Process Automation.
- Se o CA EEM usa o Active Directory, digite as suas credenciais do AD.

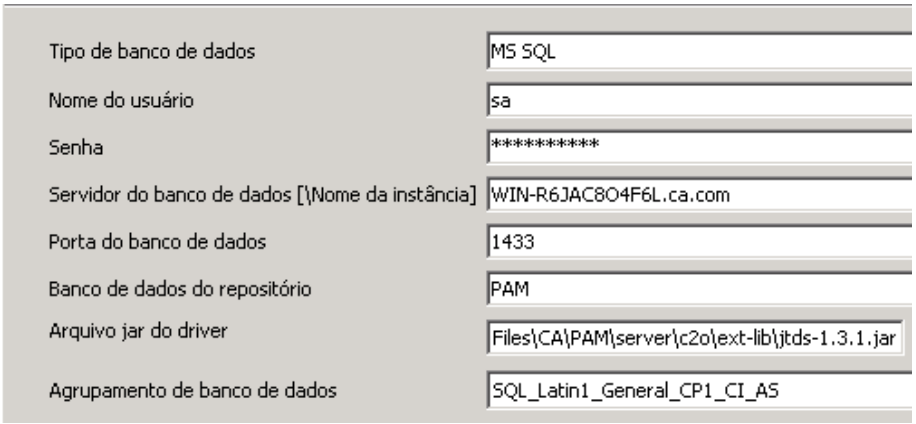
Responda à mensagem de confirmação.



16. Conforme as seguintes configurações do banco de dados forem exibidas, clique em Testar configurações do banco de dados para verificar se "Teste bem-sucedido" é exibido. Clique em Avançar.

- Banco de dados do repositório (também conhecido como o banco de dados da biblioteca)
- Banco de dados de tempo de execução
- Banco de dados de relatórios

O exemplo a seguir inclui os dados de exemplo:



17. Para obter Jars adicionais para instalação, clique em Avançar ou selecione na lista exibida e adicione outros arquivos, se necessário.
18. Aguarde enquanto a instalação atualiza (instala) o domínio do CA Process Automation.
19. Quando Concluindo o Assistente de instalação de domínio do CA Process Automation é exibido, clique em Concluir.
20. Efetue logoff do servidor no qual o nó 1 do orquestrador de domínio agrupado foi atualizado.

Observação: se tiver conectores para atualizar, adie o início do serviço do orquestrador até que essa atualização seja concluída.

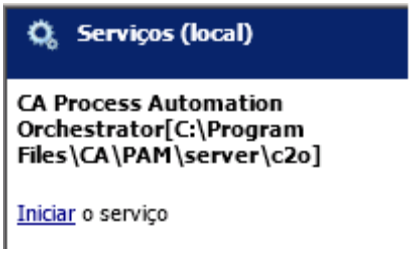
Exemplo: atualizar outro nó do orquestrador de domínio da Release 3.1 SP01 para a 4.2 no Windows

O exemplo a seguir é o segundo de dois exemplos relacionados sobre a atualização de um orquestrador de domínio agrupado da Release 3.1 SP01 para a 4.2 em um sistema operacional Windows. Os exemplos incluem instantâneos selecionados e comentários do seguinte cenário:

- Nó 1 do orquestrador de domínio - pam-sandbox-n1
- Nó 2 do orquestrador de domínio - pam-sandbox-n2
- Balanceador de carga do orquestrador de domínio - pam-sandbox-LB

Estas são as etapas:

1. Efetue logon no primeiro servidor que foi atualizado. Inicie o serviço do orquestrador por meio de Ferramentas administrativas, Serviços. Observe que o caminho é o mesmo caminho em que você inicialmente instalou o CA Process Automation.



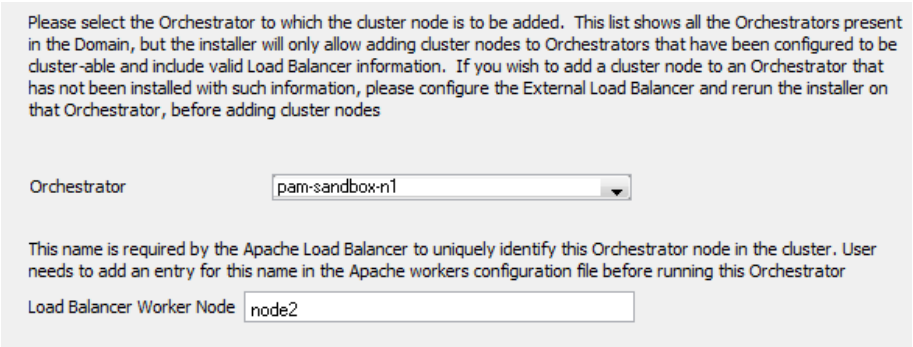
2. Efetue logon no servidor em que outro nó (por exemplo, node2) do orquestrador de domínio agrupado está instalado.
3. Vá até o URL do domínio, o balanceador de carga do orquestrador de domínio. Nesse exemplo, ele é http://pam-sandbox-lb/itpam.
4. Efetue logon, clique na guia Configuração e, em seguida, clique na paleta Instalação (lado esquerdo inferior).
5. Em Instalar o nó de agrupamento do orquestrador de domínio, clique em Instalar para iniciar a atualização.

6. A caixa de diálogo de seleção de idioma é exibida em primeiro lugar. Clique em OK.
7. Clique nas páginas seguintes do assistente:
   - Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation.
   - Contrato de Licença - selecione Eu aceito os termos do Contrato de Licença
   - Selecione o diretório de destino, C:\Arquivos de Programas\CA\PAM, por padrão.
   - Pré-requisitos para instalação do CA Process Automation - chama a instalação.
   - Concluindo o Assistente de instalação do CA Process Automation com a opção Usar domínio selecionada - Clique em Concluir

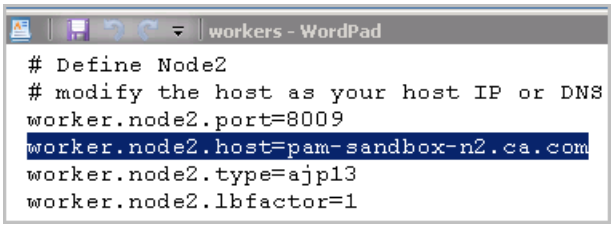
     Aguarde até que a próxima página seja exibida. Não há nenhum indicador visual do processamento que preceda a exibição da próxima página.
   - Bem-vindo ao Assistente de instalação de domínio do CA Process Automation
   - Contrato de licença
8. Se você atualizou o JDK, vá até o Diretório inicial do Java, por exemplo, C:\Arquivos de Programas\Java\jdk1.7.0_45

9. Quando a Tela de configuração for exibida,

   a. Clique na lista suspensa Orquestrador e selecione o nó do orquestrador de domínio que foi atualizado primeiro.



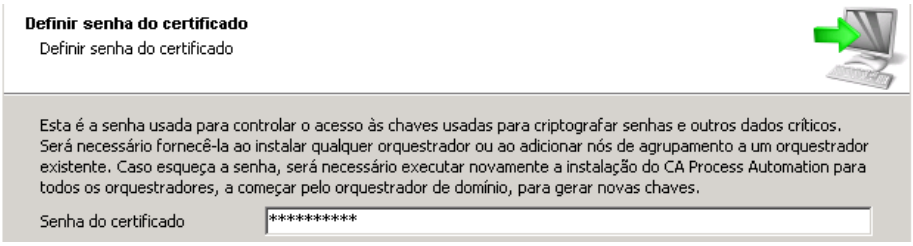
   b. Insira um valor no campo Nó de funcionário do balanceador de carga. Digite o designador para o nó (node2, node3, node4) no qual você está fazendo a atualização. Considere o formato worker.**node2**.host=*current-host*, conforme foi definido em workers.properties na pasta *apache_install_dir/conf*.



   Neste exemplo, o node2 do agrupamento do orquestrador de domínio é definido como o valor de worker.**node2**.host=pam-sandbox-n2 em workers.properties. O FQDN do balanceador de carga é previamente preenchido no campo Nome do host público.

10. Digite o nome da empresa.

11. Digite a *mesma* senha do certificado que você inseriu durante a instalação do nó anterior do orquestrador de domínio. Essa é a mesma *senha* do certificado que foi usada pelo orquestrador de domínio na release anterior.



12. Clique nas seguintes páginas, que usam as configurações do node1 neste exemplo.
    - Selecione a pasta do menu Iniciar.
    - Página Propriedades gerais (Instalar como um serviço do Windows não é mostrado, mas é suposto).
    - Diretório temporário de scripts
    - PowerShell
    - Configurações de segurança do CA Embedded Entitlements Manager CA EEM
    - Configurações do banco de dados - Repositório
    - Configurações do banco de dados - Tempo de execução
    - Configurações do banco de dados - Relatórios

    A instalação de atualização é iniciada.
13. Quando a página Concluindo o Assistente de instalação do domínio do CA Process Automation for exibida, clique em Concluir.

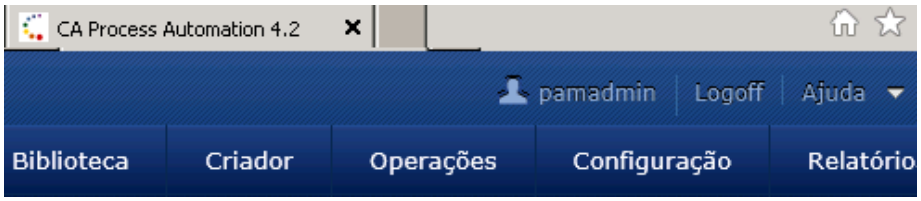
Exemplo: atualizar um orquestrador não agrupado da Release 4.1 SP01 para a 4.2 no Windows

O exemplo a seguir fornece instantâneos selecionados que se parecem com o que é visto ao atualizar um orquestrador não agrupado da Release 4.1 SP01 para a 4.2 em um sistema operacional Windows. Se não estiver familiarizado com o assistente de instalação do CA Process Automation, você pode achá-lo útil.

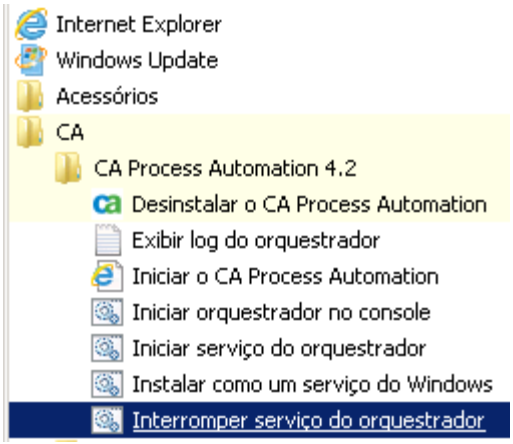
Estas são as etapas:

1. Efetue logon no host em que o Orquestrador de domínio está instalado.
2. Abra a release do CA Process Automation que está sendo atualizada. Por exemplo, no menu Iniciar, CA, CA Process Automation 4.1 SP01, Iniciar o CA Process Automation.

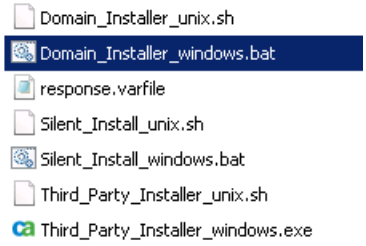
   Observação: essa é uma maneira fácil de verificar se o CA EEM está em execução e se o servidor de banco de dados está ativo. Isto é um pré-requisito para a atualização.



3. Efetue logoff do CA Process Automation, feche o navegador e interrompa o serviço do orquestrador. Por exemplo, no menu Iniciar, selecione CA, CA Process Automation 4.1 SP01, Interromper serviço do orquestrador. (Se você abrir Serviços, é possível verificar se o serviço não está com o status Iniciado.)



4. Vá até a pasta DVD1 da mídia de instalação e inicie o Domain_Installer_windows.bat.



5. Clique em Avançar para percorrer as páginas iniciais do assistente:
   - Idioma
   - Bem-vindo ao assistente de instalação do instalador de terceiros do CA Process Automation
   - Contrato de licença - Eu aceito os termos do Contrato de Licença
   - Selecionar o diretório de destino
   - Pré-requisitos para a instalação do CA Process Automation

     A instalação é iniciada, incluindo a instalação do Active MQ e a instalação de componentes de terceiros.
   - Instalação do JDBC Jars (O padrão é usar o JDBC Jars especificado durante a atualização do orquestrador de domínio.)
   - Pré-requisitos para a instalação do CA Process Automation (concluída com êxito)

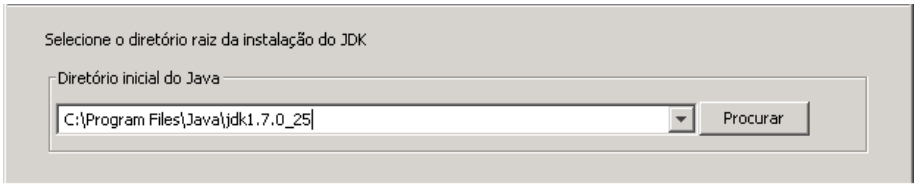
6. Quando Concluindo o Assistente de instalação do CA Process Automation é exibido, substitua DVD1 por DVD2 no caminho do diretório. Em seguida, clique em Concluir.

   A mensagem será exibida: "Copiando o instalador do CA Process Automation. Isso pode levar alguns minutos. Aguarde." Talvez haja um tempo de atraso entre o fechamento dessa página e a abertura da página de boas-vindas.

7. Quando Bem-vindo ao Assistente de instalação de domínio do CA Process Automation é exibido, clique nas páginas iniciais do assistente:

   - Idioma
   - Bem-vindo ao Assistente de instalação de domínio do CA Process Automation
   - Contrato de licença - Eu aceito os termos do Contrato de Licença

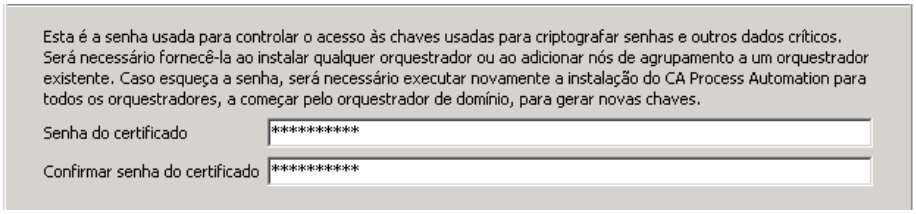
8. Para o domínio do CA Process Automation, defina o Diretório inicial do Java e vá até o diretório correto.



9. Continue clicando por meio das páginas:

   - Domínio do CA Process Automation, Reinstalar/configurar - Reinstalar é a única opção disponível para uma atualização.
   - Domínio do CA Process Automation, Tela de configuração

10. Quando Definir senha do certificado é exibido, insira a *mesma* senha do certificado que o orquestrador de domínio usa. Essa senha do certificado deve corresponder àquela inserida quando este orquestrador não agrupado foi instalado inicialmente. Clique em Avançar



11. Clique em selecionar a pasta do menu Iniciar para usar a seleção anterior.
12. Na página Propriedades gerais, observe as seguintes alterações nos padrões da porta do servidor do orquestrador:

    Porta do servidor

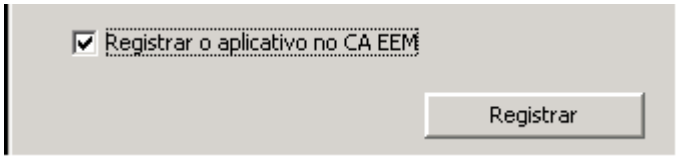
    Define a porta que o orquestrador de domínio usa para se comunicar com outros orquestradores e agentes.

    Padrão: 80 (básico: HTTP) ou 443 (protegido: HTTPS)

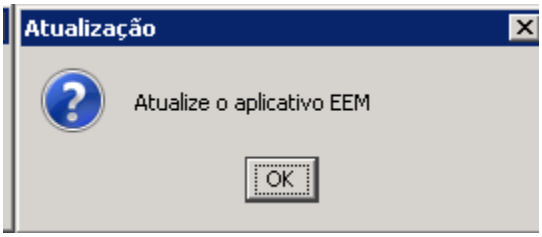
    Porta do servidor obsoleta

    (Somente atualização/reinstalação) O valor da Porta do servidor que foi definido para uma release anterior do CA Process Automation.

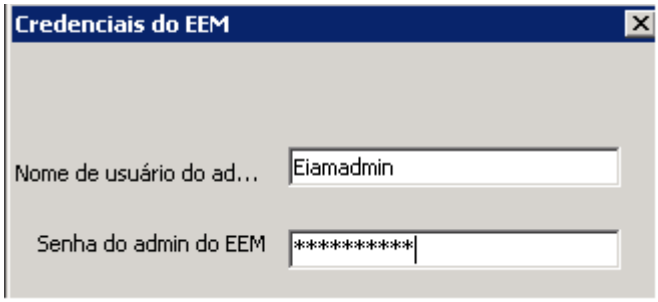
    Padrão: 7001
13. Clique nas páginas a seguir, fazendo alterações a seu critério.
    - Diretório temporário de scripts
    - Diretiva de execução do PowerShell
14. Quando Configurações de Segurança do EEM (Embedded Entitlements Manager) é exibido,
    a. Selecione Registrar o aplicativo com o CA EEM e clique em Registrar. É sempre aconselhável fazê-lo para uma atualização porque uma nova release pode conter alterações ou adições às diretivas do CA EEM para o CA Process Automation. Quando nenhuma alteração for feita entre as releases, você verá uma mensagem informando que nenhuma atualização é necessária.



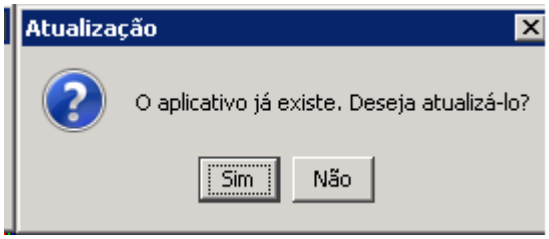
    b. Se tentar sair dessa página sem registro e o processo de instalação detectar uma atualização da versão do CA Process Automation, o processo de instalação solicitará que você selecione Registrar o aplicativo no CA EEM e, em seguida, clique em Registrar.



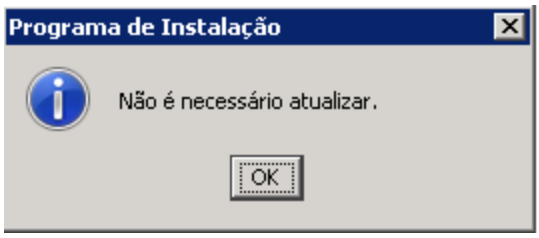
c. Forneça credenciais para efetuar logon no CA EEM como o administrador EiamAdmin.



d. Concorde com a atualização. O processo de instalação detecta a versão do servidor do CA EEM e escolhe o SDK apropriado.



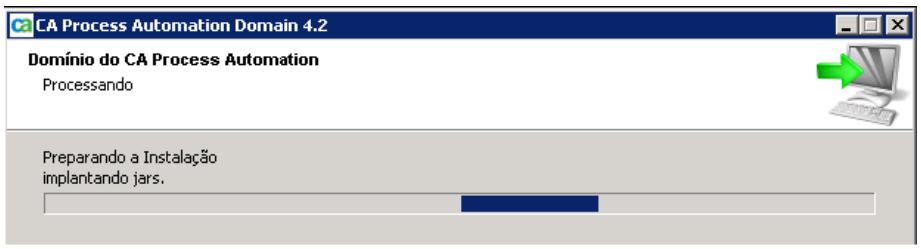
e. Se a atualização não for necessária, esta mensagem será exibida:



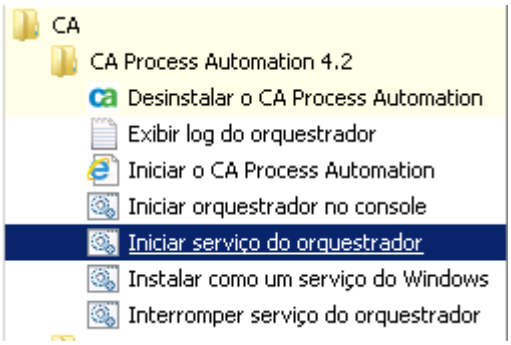
f. Clique em OK quando a confirmação de aplicativo registrado for exibida.

15. Clique nas Configurações do banco de dados, pois você já as definiu:
    - Banco de dados do repositório
    - Banco de dados de tempo de execução
    - Banco de dados de relatórios
16. Clique em Jars adicionais para instalação se não há nada a ser adicionado.

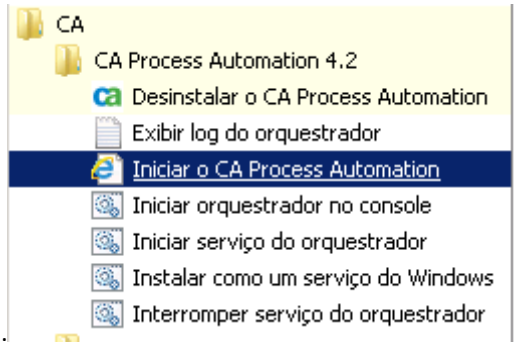
    A opção Instalação atualiza (instala) o domínio do CA Process Automation.



17. Quando Concluindo o Assistente de instalação de domínio do CA Process Automation é exibido, clique em Concluir. Dê tempo suficiente para que as atualizações do esquema sejam concluídas antes de tentar iniciar o CA Process Automation.
18. Inicie o serviço do orquestrador.



19. Inicie o CA Process Automation.



Atualizando de uma release anterior para a Release 3.1 SP01

Não é possível fazer uma atualização diretamente do CA IT Process Automation Manager (CA IT PAM) Release 2.x, Versão 3.0 ou 3.0sp01 para o CA Process Automation Release 4.2. Você deve primeiro executar uma atualização intermitente.

Siga estas etapas:

1. Atualize a partir de qualquer uma das releases anteriores para o CA Process Automation 3.1 SP01
   - CA IT PAM Release 2.x
   - CA IT PAM Versão 3
   - CA IT PAM Service Pack 3.0 SP01

   Observação: para obter informações sobre esta atualização provisória, faça download do Guia de Instalação apropriado no Atendimento ao cliente.
2. Atualize a partir do CA Process Automation Service Pack 3.1 SP01 para o CA Process Automation Release 4.2, conforme descrito em Como atualizar o CA Process Automation (na página 142).