CA ARCserve® Replication and High Availability

Guia de Instalação

r16

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA ARCserve® Replication
- CA ARCserve® High Availability (HA)
- CA ARCServe® Assured Recovery®
- CA ARCserve® Content Distribution

Em todo este guia, o termo CA ARCserve RHA é usado para representar toda a família de produtos, vendida anteriormente como CA XOsoft Replication (WANSync) e CA XOsoft High Availability (WANSyncHA).

Entrar em contato com a CA

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

As seguintes atualizações na documentação foram feitas desde a última versão desta documentação:

- Atualizado para incluir comentários do usuário, aprimoramentos, correções e outras alterações secundárias para ajudar a melhorar a utilização o e a compreensão do produto ou da documentação.

Índice

Capítulo 1: Componentes e implantação do CA ARCserve RHA

Esta seção apresenta uma visão geral dos componentes do CA ARCserve RHA e as diretrizes para uma implantação eficiente desses componentes na plataforma Microsoft Windows.

Esta seção contém os seguintes tópicos:

Componentes de replicação e alta disponibilidade

O CA ARCserve RHA consiste nos seguintes componentes:

- Serviço de controle (na página 9)
- Mecanismo (na página 10)
- Centro de gerenciamento (na página 11) - formado por três componentes: página Visão geral, Gerenciador e Centro de relatórios.
- PowerShell (na página 12)
- CA ARCserve RHA para Microsoft Failover Cluster (na página 12)

Serviço de controle

O serviço de controle funciona como único ponto de controle na operação de replicação ou de alta disponibilidade. Ele contém todo o conjunto de dados dos cenários existentes. O serviço de controle se comunica com os mecanismos e os gerenciadores. É responsável pelo gerenciamento de todas as tarefas relacionadas a cenários, como criação, configuração, monitoração e execução de cenários.

O serviço de controle recebe solicitações dos gerenciadores, processa essas solicitações, converte-as em determinados comandos que, em seguida, transmite para os mecanismos. O serviço de controle recebe dados e eventos atualizados dos mecanismos e devolve para o gerenciador as informações e as estatísticas sobre o estado do cenário.

O Serviço de controle também é responsável pela autenticação e autorização de usuários. Age também como ponto central para o controle e o armazenamento de relatórios. Para apresentar ao usuário informações e estatísticas acumuladas pelo serviço de controle, use a página Visão geral, o gerenciador, o Centro de relatórios e o PowerShell.

Todos os arquivos de cenários são mantidos no servidor que executa o Serviço de controle. Quando o Serviço de controle está desativado, o funcionamento do cenário não é afetado. Porém, para receber informações sobre o estado do cenário, o Serviço de controle deverá estar ativado. Para obter melhores resultados, instale o serviço de controle em um host autônomo. Se isso não for possível, você pode instalar o serviço de controle nos servidores mestre ou de réplica. Entretanto, se o servidor estiver inativo, a conexão com o serviço de controle será perdida e não será possível gerenciar os cenários serão impossíveis.

Você pode proteger o Serviço de controle do CA ARCserve RHA em cenários separados. Para obter informações, consulte Protegendo o serviço de controle no *Guia de Administração do CA ARCserve RHA*.

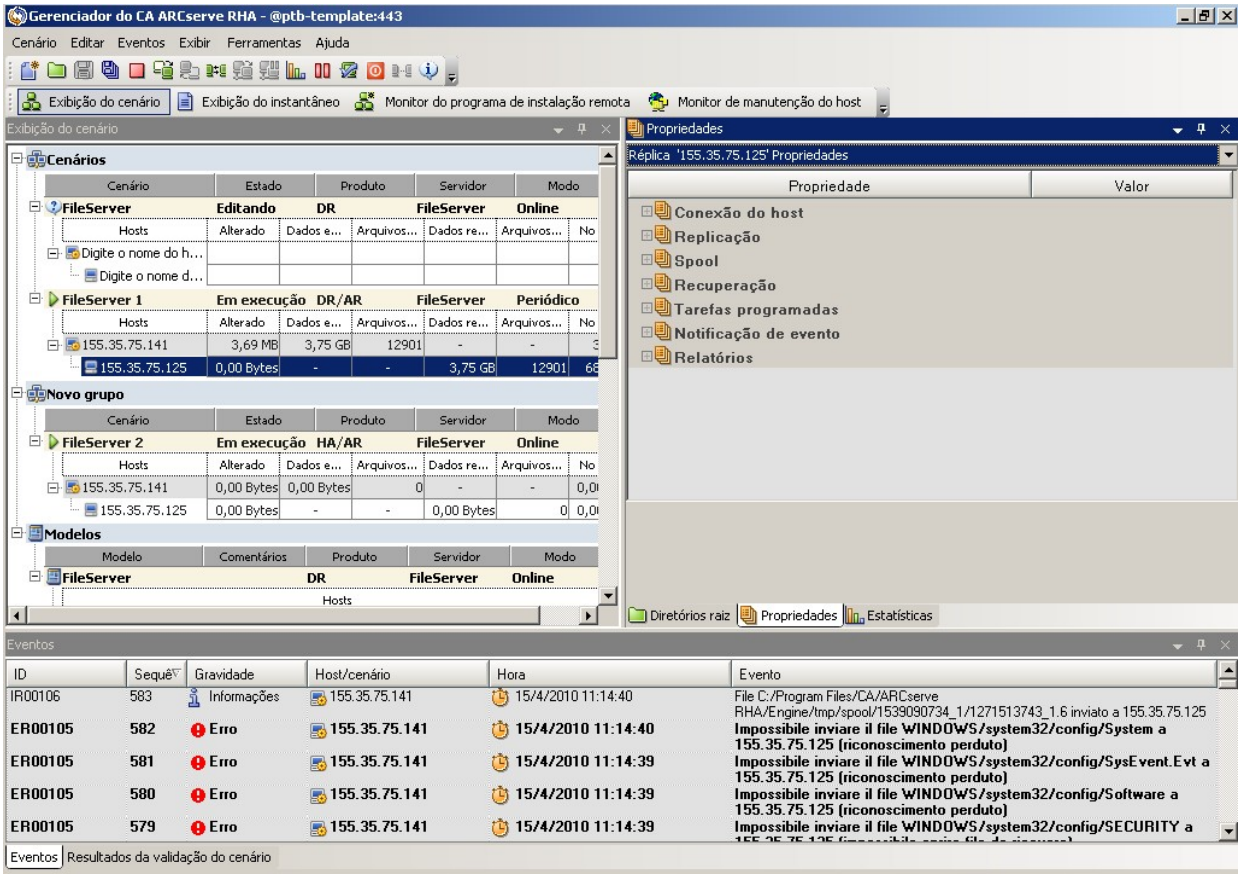
Mecanismo

O mecanismo é um serviço que deve estar em execução antes do início de qualquer cenário. É instalado em todos os servidores que fazem parte do cenário determinado, abrangendo os hosts Mestre (origem) e de Réplica (destino). Cada mecanismo aceita as funcionalidades do mestre e da réplica, para os cenários Recuperação de falhas e Alta disponibilidade. Pode participar de vários cenários e executar uma função diferente em cada cenário. Os mecanismos podem ser instalados localmente em um host por vez ou por meio de um programa de instalação remoto em vários hosts de uma vez, além de poderem ser instalados durante a criação do cenário, se necessário.

Centro de gerenciamento

O Centro de gerenciamento é formado por três componentes, sendo que nenhum deles exige instalação manual:

- **Página Visão geral** - visão geral estatística do estado dos cenários Recuperação de falhas e Alta disponibilidade.
- **Gerenciador** - interface de usuário que permite criar, configurar, gerenciar e monitorar cenários. Este é um aplicativo de GUI, ativado na página Visão geral com um clique no link Gerenciamento de cenário.



- **Centro de relatórios** - interface de usuário que reúne todos os relatórios existentes, juntamente com informações sobre os relatórios disponíveis em cada cenário. Você decide em que local esses relatórios serão armazenados e até quando serão exibidos e salvos no Centro de relatórios.

PowerShell

O PowerShell é oferecido como alternativa, caso não deseje gerenciar o processo de replicação usando a interface gráfica do Gerenciador. Ele amplia e facilita os recursos do CLI fornecidos em versões anteriores e oferece suporte às operações de replicação e alta disponibilidade.

O PowerShell é um shell de linha de comando e um ambiente de script que permite aos usuários configurar cenários de replicação, além de controlar e monitorar o processo de replicação. Todos os cenários gerenciados pelo PowerShell têm aparência e funcionamento exatamente iguais aos cenários controlados pelo gerenciador e são salvos automaticamente no mesmo local padrão: INSTALL_DIR/ws_scenarios.

O PowerShell tem como base o Windows PowerShell™ padrão, fornecido com um amplo conjunto de comandos incorporados e interface consistente. O componente PowerShell adiciona uma série de comandos relacionados aos cenários, chamada snap-ins, que facilitam o gerenciamento.

CA ARCserve RHA para Microsoft Failover Cluster

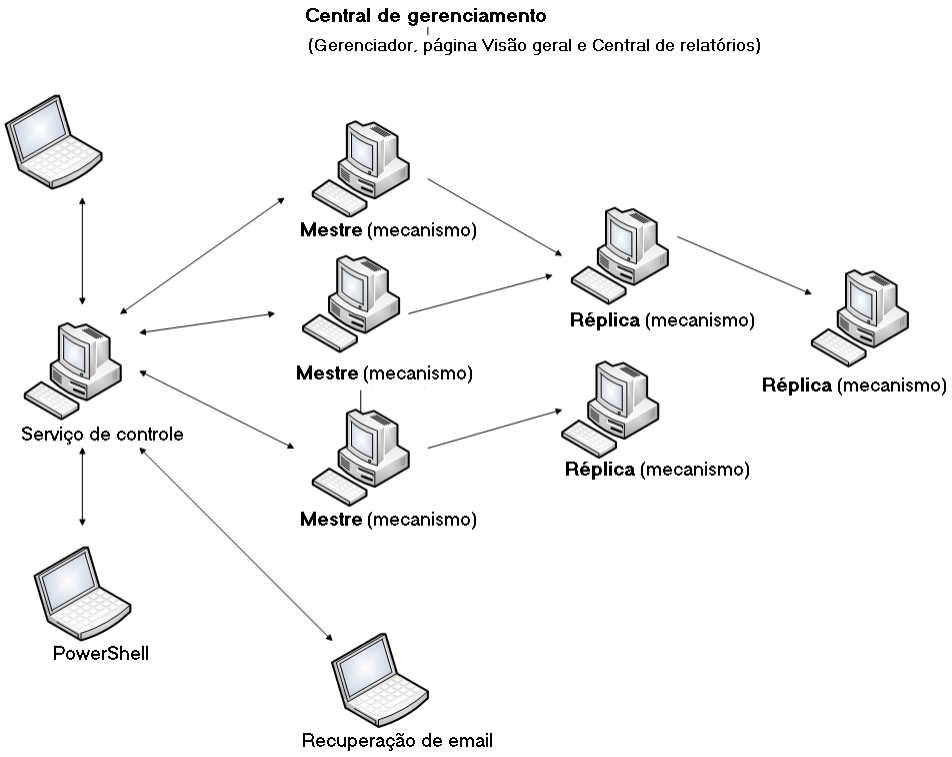
O CA ARCserve RHA para Microsoft Failover Cluster inclui um plug-in para o recurso de disco virtual e uma interface leve instalada em cada nó do agrupamento.

Embora a alta disponibilidade esteja integrada aos ambientes de agrupamento da Microsoft, o armazenamento compartilhado ainda pode ser um único ponto de falha. O CA ARCserve RHA protege o armazenamento de agrupamento, permitindo replicar dados em um recurso de disco, localmente ou não.

Implantação do CA ARCserve RHA

A implantação dos componentes do CA ARCserve RHA depende do tamanho da rede corporativa de TI e das necessidades de replicação e alta disponibilidade. Entretanto, há algumas diretrizes que devem ser observadas ao planejar seu ambiente de replicação e alta disponibilidade e implantar diferentes componentes do CA ARCserve RHA em uma plataforma Windows. A próxima seção apresenta informações sobre a implantação eficiente de componentes do CA ARCserve RHA.

A ilustração a seguir mostra uma implantação típica de componentes do CA ARCserve RHA:



- **Serviço de controle do CA ARCserve RHA**

  O serviço de controle deve estabelecer conexão com todos os servidores mestre e de réplica de alternância. Não é obrigatório que o serviço de controle tenha uma conexão direta para cada servidor que não seja de réplica de alternância nos cenários.

  É recomendável instalar o serviço de controle em um servidor separado. Se estiver trabalhando com cenários de alta disponibilidade, não instale o serviço de controle nos hosts mestre ou de réplica.

É possível instalá-lo na estação de trabalho local. Porém, lembre-se de que, se a estação de trabalho estiver desativada ou offline, não será possível monitorar nem gerenciar cenários.

- **Mecanismo do CA ARCserve RHA**

  O mecanismo deve ser instalado em cada servidor mestre e de réplica que participe dos cenários definidos.

- **Centro de gerenciamento do CA ARCserve RHA**

  É possível abrir esse componente em qualquer estação de trabalho que tenha um navegador e conectividade de rede ao serviço de controle.

- **CA ARCserve RHA PowerShell**

  É possível abrir esse componente em qualquer estação de trabalho que tenha o Windows PowerShell e conectividade de rede ao serviço de controle.

Capítulo 2: Requisitos e configurações dos componentes do CA ARCserve RHA

Esta seção fornece informações sobre os requisitos de software e configuração de cada componente do CA ARCserve RHA.

Observação: para obter a lista mais atualizada dos sistemas operacionais suportados, consulte as Notas da Versão ou acesse o site da CA em arcserve.com.

Esta seção contém os seguintes tópicos:

Requisitos do serviço de controle

Sistemas operacionais

- Windows Server 2003 de 32 e 64 bits
- Windows Server 2003 R2 de 32 e 64 bits
- Windows Server 2008 de 32 e 64 bits
- Windows Server 2008 R2

Observação: para evitar erros de configuração da Microsoft, instale o serviço de controle em sistemas Windows Server 2003 e Windows Server 2008 R2 usando a conta de administrador, caso queira implantar o mecanismo em hosts locais usando o programa de instalação remota.

Importante! durante a instalação do serviço de controle, ao fornecer as informações de logon no serviço, é possível usar a conta de administrador ou definir uma nova conta. Se definir uma nova conta, o estado de inicialização do serviço de navegador de computadores do sistema operacional deve ser de Ativado, e o serviço precisa estar em execução. No Windows Server 2003, o serviço de navegador de computadores é ativado por padrão, mas no Windows Server 2008, o estado de inicialização deste serviço é **desativado** por padrão. Portanto, se você deseja instalar o serviço de controle no Windows 2008 e definir uma nova conta de sistema, antes de iniciar a instalação, é necessário alterar o estado de inicialização do serviço de navegador de computadores para **Automático** e, em seguida, iniciar o serviço. Como o serviço de navegador de computadores se baseia em compartilhamento de arquivos e impressora, também é necessário ativar o **Compartilhamento de arquivos e impressoras** na Central de redes e compartilhamento. Para obter mais informações sobre ativação do estado de inicialização do serviço de navegador de computadores, consulte o site da Microsoft http://technet.microsoft.com/en-us/library/bb726965.aspx.

Após o término da instalação, será possível interromper o serviço de navegador de computadores e **desativar** novamente o estado de inicialização.

Há vários aplicativos obrigatórios que serão incluídos automaticamente durante o processo de instalação, se ainda não estiverem instalados no computador. Esses aplicativos incluem:

- Microsoft .NET Framework Versão 2.0
- Microsoft ASP.NET 2.0 AJAX Extensions 1.0
- Microsoft Core XML Services 6.0

Credenciais do usuário

- Um usuário Windows que executa o serviço de controle do CA ARCserve RHA precisa ter permissão de leitura e gravação no diretório de instalação.

Requisitos do Mecanismo

O componente Mecanismo é compatível com estes sistemas operacionais:

- Windows Server 2003 de 32 e 64 bits
- Windows Server 2003 R2 de 32 e 64 bits
- Windows Server 2008 de 32 e 64 bits
- Windows Server 2008 R2 incluindo a instalação do Server Core
- AIX
- Solaris
- Red Hat Linux
- SuSE Linux
- CentOS

Importante: durante a instalação do mecanismo, ao fornecer as informações de logon no serviço, é possível usar a conta de administrador ou definir uma nova conta. Se definir uma nova conta, o estado de inicialização do serviço de navegador de computadores do sistema operacional deve ser de Ativado, e o serviço precisa estar em execução. No Windows Server 2003, o serviço de navegador de computadores é ativado por padrão, mas no Windows Server 2008, o estado de inicialização deste serviço é **desativado** por padrão. Portanto, se deseja instalar o mecanismo no Windows 2008 e definir uma nova conta de sistema, antes de iniciar a instalação, é necessário alterar o estado de inicialização do serviço de navegador de computadores para **Automático** e, em seguida, iniciar o serviço. Como o serviço de navegador de computadores se baseia em compartilhamento de arquivos e impressora, também é necessário ativar o **Compartilhamento de arquivos e impressoras** na Central de redes e compartilhamento. Para obter mais informações sobre ativação do estado de inicialização do serviço de navegador de computadores, consulte o site da Microsoft http://technet.microsoft.com/en-us/library/bb726965.aspx.

Após o término da instalação, será possível interromper o serviço de navegador de computadores e **desativar** novamente o estado de inicialização.

Requisitos do Centro de gerenciamento

Navegador web

- Internet Explorer versão 6, 7, 8 ou 9.

  Observação: autorize o script ativo no seu navegador.

Conta de logon

- Para efetuar logon no Centro de gerenciamento, você deve ser integrante do grupo de administradores no computador local onde o serviço de controle está instalado.

Requisitos do PowerShell

Sistemas operacionais

- Windows Server 2003 de 32 e 64 bits
- Windows Server 2003 R2 de 32 e 64 bits
- Windows Server 2008 de 32 e 64 bits
- Windows Server 2008 R2
- Windows Server 2008 de 32 e 64 bits
- Windows Vista
- Windows XP

.Net Framework

- Microsoft .NET Framework 2.0. (build 50727)

O .Net Framework é necessário para a instalação do Windows PowerShell. Baixe o aplicativo no Centro de Download da Microsoft e instale-o.

Microsoft PowerShell

- Microsoft PowerShell versão 1.0

O Windows Vista SP1 contém o PowerShell como aplicativo incorporado. Se usar o Windows XP ou 2003, baixe e instale diretamente da Microsoft.

Requisitos de sistema do agrupamento

Verifique se o Microsoft Windows 2003, 2008 e 2008 R2 estão instalados em todos os computadores do agrupamento. Os agrupamentos típicos consistem em 5 (cinco) máquinas:

- Windows Server 2008 R2 Failover Cluster (x64) como controlador de domínio e um servidor DNS.
- Algumas máquinas virtuais executando o Windows 2008 R2 (x64), associado ao mesmo domínio controlado pelo primeiro servidor.
- Uma quinta máquina executando o FreeNAS.
- Microsoft .NET Framework 3.5 (ou mais recente) em todos os nós do agrupamento.

Importante: Os dados e logs do aplicativo devem residir no mesmo volume.

Para obter mais informações, consulte a documentação da Microsoft para ter certeza de que seu ambiente de agrupamento está configurado corretamente.

Capítulo 3: Requisitos de aplicativos e bancos de dados suportados

Esta seção fornece informações sobre os requisitos de configuração e de conta de logon de cada servidor de aplicativos e banco de dados suportados e de cada solução de replicação.

Observação: os requisitos e as configurações de um servidor de arquivos estão descritos na seção Instalando o mecanismo do CA ARCserve RHA (na página 79).

Esta seção contém os seguintes tópicos:

Servidores de aplicativos e bancos de dados suportados

As soluções de replicação e alta disponibilidade são ajustadas e personalizadas para os seguintes servidores de aplicativos e bancos de dados do Windows de 32 e 64 bits:

- Servidor de arquivos
- Microsoft Exchange
- Microsoft SQL
- Microsoft IIS
- Oracle
- Microsoft SharePoint
- Microsoft Hyper-V
- VMware vCenter Server
- Serviço de controle do CA ARCserve RHA
- Microsoft Dynamics CRM

O CA ARCserve RHA também pode transferir sistema completos para máquinas virtuais. Para obter uma lista atualizada de plataformas e aplicativos compatíveis, consulte o documento *CA ARCserve RHA Supported Configurations*, no site do suporte da CA.

Importante: para obter todos os servidores suportados, atribua estaticamente todos os endereços IP (endereços IP atribuídos pelo DHCP no servidor mestre ou de réplica não são suportados).

Replicação e alta disponibilidade do servidor de arquivos

Esta seção descreve os requisitos para execução do CA ARCserve RHA no servidor de arquivos.

Requisitos do servidor de arquivos

Para implementar os procedimentos de alta disponibilidade para servidor de arquivos, é necessário ter as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- (No mesmo ambiente do diretório ativo) os servidores mestre e de réplica devem residir na mesma floresta do diretório ativo e ser integrantes do mesmo domínio ou de domínios confiáveis.
- Atribuir estaticamente todos os endereços IP (não há suporte para endereços IP atribuídos a DHCP no servidor mestre ou de réplica).
- O servidor protegido não é um controlador de domínios ou servidor DNS.

Conta de logon no servidor de arquivos

A conta de logon de serviço do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, use uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.

Operação de servidores de arquivos em um grupo de trabalho

Para servidores em um grupo de trabalho, defina a conta de serviço do mecanismo do CA ARCserve RHA como Sistema local (a menos que você tenha adicionado algum script personalizado que exija permissões de nível superior). Servidores em um grupo de trabalho podem usar Redirecionar DNS somente com servidores DNS que permitem atualizações sem segurança. Você pode usar normalmente os redirecionamentos Mover IP, Alterar o nome do computador e Scripts de redirecionamento personalizados.

Replicação e alta disponibilidade do Microsoft Exchange Server

Esta seção descreve os requisitos de configuração do CA ARCserve RHA para o Microsoft Exchange Server.

Replicação do Exchange Server

Esta seção descreve os requisitos para execução do CA ARCserve RHA no Exchange Server.

Configuração de replicação do Exchange

Para implementar a replicação no Exchange Server, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Servidor Exchange instalado nos servidores mestre e de réplica, com a mesma edição, versão, service packs e hot fixes instaladas.
- Exchange Server instalado com as mesmas credenciais de logon nos servidores mestre e de réplica.
- Os dois servidores devem ter a caixa de correio e as funções de CAS instaladas. Se o servidor mestre for o único servidor na organização do Exchange que apresente as funções de transferência de CAS e HUB, o servidor de réplica deve apresentar as mesmas funções do Exchange Server instaladas.
- Os dois servidores devem apresentar a mesma versão do PowerShell instalada.
- Os dois servidores devem apresentar o mesmo grupo administrativo do Exchange.

Observação: o Exchange Server 2010 não permite criar dois bancos de dados com o mesmo nome em servidores mestre e de réplica, mesmo se o banco de dados estiver desmontado. Use um nome para o banco de dados de réplica, que seja menor do que 64 caracteres e siga a seguinte convenção:

<ReplicaName>=<MasterName>_xxxx

Em que xxx = número aleatório.

Conta de logon da replicação do Exchange

A conta de logon do serviço do mecanismo do CA ARCserve RHA deve atender a todas estas condições:

- Deve ser uma conta Exibição do Exchange apenas de administrador.
- Deve ser integrante do grupo Administradores na máquina local.

Observação: se a política de segurança de sua empresa exige permissões ainda mais granulares que as descritas, entre em contato com o suporte técnico da CA para receber instruções detalhadas sobre as permissões necessárias.

Agrupamentos de replicação do Exchange

Com o CA ARCserve RHA, trabalhar com agrupamentos é quase idêntico a trabalhar com servidores autônomos. 'asta inserir o "Nome do servidor virtual do Exchange" como nome do servidor Mestre ou de Réplica, no local adequado.

No Exchange 2007, o CA ARCserve RHA oferece suporte a implantações de LCR. Nenhuma configuração adicional é necessária.

Observação: no Exchange 2007, não há suporte para implantações de CCR.

Alta disponibilidade para Exchange Server

Esta seção descreve os requisitos para execução do CA ARCserve HA para Exchange Server.

Configuração de HA do Exchange

Para implementar a replicação no Exchange Server, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Servidor Exchange instalado nos servidores mestre e de réplica, com a mesma edição, versão, service packs e hot fixes instaladas.
- Exchange Server instalado com as mesmas credenciais de logon nos servidores mestre e de réplica.
- Os dois servidores devem ter a caixa de correio e as funções de CAS instaladas. Se o servidor mestre for o único servidor na organização do Exchange que apresente as funções de transferência de CAS e HUB, o servidor de réplica deve apresentar as mesmas funções do Exchange Server instaladas.
- Os dois servidores devem apresentar a mesma versão do PowerShell instalada.
- Os dois servidores devem apresentar o mesmo grupo administrativo do Exchange.

Observação: o Exchange Server 2010 não permite criar dois bancos de dados com o mesmo nome em servidores mestre e de réplica, mesmo se o banco de dados estiver desmontado. Use um nome para o banco de dados de réplica, que seja menor do que 64 caracteres e siga a seguinte convenção:

<ReplicaName>=<MasterName>_xxxx

Em que xxx = número aleatório.

Conta de logon de HA do Exchange

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo Administradores de domínios.
- Deve ser administrador do Exchange.
- Deve ser integrante do grupo Administradores no computador local.

Observação: se a política de segurança de sua empresa exige permissões mais granulares que as descritas, entre em contato com o suporte técnico do CA ARCserve RHA para receber instruções detalhadas sobre as permissões necessárias.

Agrupamentos de alta disponibilidade do Exchange Server

No CA ARCserve Replication, trabalhar com agrupamentos é quase idêntico a trabalhar com servidores independentes. 'asta inserir o "Nome do servidor virtual do Exchange" como nome do servidor Mestre ou de Réplica, no local adequado.

No Exchange 2007, o CA ARCserve HA oferece suporte a implantações de LCR. Nenhuma configuração adicional é necessária.

Observação: no Exchange 2007, implantações de CCR não são suportadas.

Replicação e alta disponibilidade do Microsoft SQL Server

Esta seção descreve os requisitos do CA ARCserve RHA para o Microsoft SQL Server.

Replicação do SQL Server

Esta seção descreve os requisitos para execução do CA ARCserve RHA no SQL Server.

Configuração de replicação do SQL

Para implementar a replicação no SQL Server, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Uma sessão do SQL Server instalada no mestre.

Para usar a solução de replicação com a opção de **Recuperação garantida** para SQL Server, você precisa ter as seguintes configurações:

- A mesma versão do Microsoft SQL Server instalada nos servidores mestre e de réplica.
- SQL Server instalado com as mesmas credenciais de logon nos servidores mestre e de réplica.

Além disso, você deve interromper o serviço do SQL Server no host de Réplica, quando a replicação está ativa.

Observação: se o banco de dados mestre do SQL não estiver replicado, você poderá remover os bancos de dados replicados no servidor de réplica sem interromper o serviço do mecanismo.

Conta de logon da replicação do SQL

A conta de logon do serviço do mecanismo do CA ARCserve RHA deve atender a todas estas condições:

- Para servidores independentes (isto é, não agrupados), use o padrão do sistema local.
- Para nós de agrupamento, use a conta de serviço de um administrador local em todos os nós agrupados.

Alta disponibilidade para SQL Server

Esta seção descreve os requisitos para execução do CA ARCserve HA para SQL Server.

Configuração de HA do SQL

Para implementar procedimentos de Alta disponibilidade para SQL Server, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Uma ou mais sessões do Microsoft SQL Server instaladas em cada servidor:
  - Os dois servidores devem ter as mesmas versões de SQL, service packs e hot fixes instaladas.
  - Os dois servidores devem manter sessões idênticas do SQL Server, isto é, padrão ou nomeada.
  - As letras de unidades que contêm arquivos de bancos de dados devem ser idênticas nos dois servidores.
  - O caminho completo do banco de dados padrão do sistema de cada sessão deve ser idêntico nos dois servidores.
  - (No ambiente do diretório ativo) os servidores mestre e de réplica devem residir na mesma floresta do diretório ativo e ser integrantes do mesmo domínio ou de domínios confiáveis.
- Verifique se a porta definida nas propriedades TCP/IP de configuração da rede, das sessões de SQL, foi atribuída estaticamente e se é idêntica nos servidores mestre e de réplica.
- O servidor protegido não é um controlador de domínios ou servidor DNS.

Conta de logon no HA do SQL

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, será necessário usar uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.
- Se a conta não possuir permissões de Administrador incorporadas em todas as sessões do SQL Server, adicione as permissões adequadas.

Observação: se a política de segurança de sua empresa exige permissões mais granulares que as descritas, entre em contato com o suporte técnico para receber instruções detalhadas. Para servidores em um grupo de trabalho, mantenha o usuário de logon como sistema local.

Operação de SQL Servers em um grupo de trabalho

Para servidores em um grupo de trabalho, defina a conta do serviço mecanismo do CA ARCserve HA para um usuário que seja integrante do grupo de administradores locais. Servidores em um grupo de trabalho podem usar Redirecionar DNS somente com servidores DNS que permitem atualizações sem segurança. Você pode usar normalmente os redirecionamentos Mover IP, Alterar o nome do computador e Scripts de redirecionamento personalizados.

Quando a opção Alterar o nome do computador é usada, você pode usar a conta de sistema ou o grupo de administradores locais, desde que a conta tenha sido adicionada aos logons do Microsoft SQL.

Agrupamentos de alta disponibilidade do SQL

Para instalação em um agrupamento, insira o nome do servidor virtual do SQL Server como o nome do servidor mestre ou de réplica.

A única configuração que exige alguma preparação é o uso de Mover IP em conjunto com um agrupamento. Para obter instruções detalhadas sobre como usar a opção Mover IP com agrupamentos, consulte o *Guia de Operações para Microsoft SQL do CA ARCserve RHA*.

Alta disponibilidade para IIS Server

Esta seção descreve os requisitos para execução do CA ARCserve HA para Microsoft IIS Server.

Configurações de HA do IIS

Para implementar procedimentos de alta disponibilidade, usando o servidor IIS do CA ARCserve HA, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

  - Service packs e hot fixes de mesmo nível devem estar instalados nos dois servidores.
  - (No ambiente do diretório ativo) os servidores mestre e de réplica devem residir na mesma floresta do diretório ativo e ser integrantes do mesmo domínio ou de domínios confiáveis.
- Uma instância do Microsoft IIS Server 6.0, 7.0 ou 7.5 instalada em cada servidor:
  - Os dois servidores devem ter instalados os mesmos serviços do IIS: WWW, SMTP etc.
  - Os dois servidores devem ter instaladas extensões idênticas de serviços da Web.
  - Os caminhos completos contendo arquivos de site devem ser idênticos nos dois servidores.
- O servidor em espera deve manter uma instalação simples do IIS, apenas com os sites padrão.
- Os sites no servidor mestre não devem usar redirecionamento de URL nem caminho UNC.

- Se o acesso anônimo for ativado e utilizado, configure o seguinte:

  Para manter permissões sincronizadas nos dois servidores, os dois processos de IIS devem utilizar a mesma conta de usuário para acesso anônimo. Crie uma nova conta de usuário do domínio e configure os dois servidores IIS para usá-la. Os próximos documentos descrevem como fazê-lo:

  - Para IIS 6.0: *Como configurar autenticação de site Web do IIS no Windows Server 2003* http://support.microsoft.com/kb/324274
  - Para IIS 7.0/7.5: *Configure a Anonymous Authentication Identity (IIS 7)* http://technet.microsoft.com/en-us/library/cc770966

    Observação: embora o documentos não especifiquem, é necessário editar a política de grupo Local (ou Domínio) para fornecer à conta do usuário os seguintes privilégios: Permitir logon localmente, Permitir logon como uma tarefa em lote e Acessar este computador na rede. Além disso, certifique-se de que todas as mudanças de permissão realizadas no sistema de arquivos para a conta original de usuário anônimo sejam duplicadas para a conta de domínio atribuída recentemente.

- No IIS 6.0, 7.0/7.5, se definir novos pools de aplicativos no servidor mestre, deverá também definí-los no servidor de réplica.
- Se usar criptografia SSL, consulte os documentos da Microsoft a seguir referentes à cópia do certificado adequado:
  - Para IIS 6.0: *Como carregar saldo um farm de servidores Web usando um certificado SSL no IIS 6.0 e no IIS 5.0* em http://support.microsoft.com/kb/313299
  - Para IIS 7.0/7.5: *instalando IIS 7.0* em http://technet.microsoft.com/en-us/library/cc268245.aspx
- O servidor protegido não é um controlador de domínios ou servidor DNS.
- Se estiver usando o IIS 7.0/7.5, é necessário ter o Management Compatibility do IIS 6.0 instalado. Como o IIS 6.0 Management Compatibility é desativado por padrão durante a instalação do IIS 7.0/7.5, é preciso ativar essa opção durante o processo de instalação do IIS 7.0/7.5.

Conta de logon no HA do IIS

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, use uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.
- Para servidores em um grupo de trabalho, use a conta de sistema local.

Observação: se a política de segurança de sua empresa exige permissões mais granulares que as descritas, entre em contato com o suporte técnico para receber instruções detalhadas. Considerações especiais se aplicam a servidores IIS operando em grupos de trabalho: consulte o Guia de Operação para obter mais informações.

Alta disponibilidade para Oracle Server

Esta seção descreve os requisitos para execução do CA ARCserve HA para o servidor Oracle.

Configurações de HA do Oracle

Para implementar procedimentos de alta disponibilidade, usando o servidor Oracle do CA ARCserve HA, você precisará das seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

  - Service packs e hot fixes de mesmo nível devem estar instalados nos dois servidores.
- Service packs e hot fixes de mesmo nível devem estar instalados nos dois servidores.
- (No ambiente do diretório ativo) os servidores mestre e de réplica devem residir na mesma floresta do diretório ativo e ser integrantes do mesmo domínio ou de domínios confiáveis.
- A SID do Oracle deve ser idêntica nos servidores mestre e de réplica.
- Nos dois servidores, verifique se todos os serviços do Oracle, normalmente carregados na inicialização, foram iniciados com êxito e estão configurados para inicialização automática.
- O caminho do diretório ORACLE_HOME e o caminho dos arquivos de banco de dados nos servidores mestre e de réplica devem ser idênticos.
- Para minimizar o tráfego de replicação, espaços de tabelas temporários do Oracle são excluídos da replicação (verifique se o banco de dados do Oracle no servidor de réplica está configurado com os mesmos nomes de espaços de tabelas temporários e os mesmos caminhos utilizados no servidor mestre).
- Nos dois servidores, configure o Oracle para montar o banco de dados automaticamente na inicialização do serviço (oradim -edit -sid ORACLE_SID -startmode auto).
- O servidor protegido não é um controlador de domínios ou servidor DNS.

Em sistemas UNIX e Linux, o CA ARCserve RHA requer o Oracle Instant Client de 32 bits para oferecer suporte aos bancos de dados Oracle. Caso não tenha esse cliente instalado, cancele a instalação do CA ARCserve RHA, faça download do Oracle Instant Client a partir do site da Oracle e reinicie a instalação do CA ARCserve RHA. Se o Instant Client já estiver instalado, é necessário fornecer o caminho completo de instalação manualmente.

Conta de logon no HA do Oracle

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, use uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.

Observação: se a política de segurança de sua empresa exige permissões mais granulares que as descritas, entre em contato com o suporte técnico para receber instruções detalhadas.

Operação de servidores Oracle em grupos de trabalho

Para servidores em um grupo de trabalho, defina a conta de serviço do mecanismo para um usuário que seja integrante do grupo de administradores locais. Servidores em um grupo de trabalho podem usar Redirecionar DNS somente com servidores DNS que permitem atualizações sem segurança. Você pode usar normalmente os redirecionamentos Mover IP, Alterar o nome do computador e Scripts de redirecionamento personalizados.

Replicação e alta disponibilidade do Microsoft Hyper-V Server

Replicação do Hyper-V Server

Esta seção descreve os requisitos para execução do CA ARCserve RHA para Hyper-V Server.

Configuração de replicação do Hyper-V

Para implementar a replicação no Hyper-V Server, são necessárias as seguintes configurações:

- O mestre em execução no Windows Server.
- A réplica em execução no Windows Server.
- Uma sessão do Hyper-V Server instalada no mestre.

Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

Conta de logon da replicação do Hyper-V

A conta de logon do serviço do mecanismo do CA ARCserve RHA deve atender a todas estas condições:

- Para servidores independentes (isto é, não agrupados), use o padrão do sistema local.
- Para nós de agrupamento, use a conta de serviço de um administrador local em todos os nós agrupados.

Alta disponibilidade para Hyper-V

Esta seção descreve os requisitos para execução do CA ARCserve HA para Hyper-V Server.

Configuração de alta disponibilidade do Hyper-V

Para implementar procedimentos de Alta disponibilidade para Hyper-V Server, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Os dois servidores devem ter as mesmas versões de Hyper-V, service packs e hot fixes instaladas.
- (No ambiente do diretório ativo) os servidores mestre e de réplica devem residir na mesma floresta do diretório ativo e ser integrantes do mesmo domínio ou de domínios confiáveis.
- Atribuir estaticamente todos os endereços IP (não há suporte para endereços IP atribuídos a DHCP no servidor mestre ou de réplica).
- O servidor protegido não é um controlador de domínios ou servidor DNS.

Não use o caminho de instalação padrão do Hyper-V. Em vez disso, crie uma pasta, como C:\vm\ no mestre e na réplica. O CA ARCserve RHA não pode acessar o caminho de instalação da máquina virtual padrão durante a detecção automática.

Conta de logon de HA do Hyper-V

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, use uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.
- Para servidores em um grupo de trabalho, use a Conta de sistema local.

Replicação e alta disponibilidade do Microsoft SharePoint Server

Replicação para o SharePoint Server

Esta seção descreve os requisitos para execução do CA ARCserve RHA no SharePoint Server.

Configuração de replicação do SharePoint

Para implementar a replicação no SharePoint Server, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Uma sessão do SharePoint Server instalada no mestre.

Para usar a solução de replicação com a opção de **Recuperação garantida** para SharePoint Server, você precisa ter as seguintes configurações:

- A mesma versão do SharePoint Server instalada nos servidores mestre e de réplica.
- SharePoint Server instalado com as mesmas credenciais de logon nos servidores mestre e de réplica.

Conta de logon da replicação do SharePoint

A conta de logon do serviço do mecanismo do CA ARCserve RHA deve atender a todas estas condições:

- Para servidores independentes (isto é, não agrupados), use o padrão do sistema local.
- Para nós de agrupamento, use a conta de serviço de um administrador local em todos os nós agrupados.

Alta disponibilidade para SharePoint Server

Esta seção descreve os requisitos para execução do CA ARCserve HA para SharePoint Server.

Configuração de alta disponibilidade do SharePoint

Para implementar procedimentos de Alta disponibilidade para SharePoint Server, são necessárias as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Uma instância do SharePoint Server instalado em cada servidor:
  - Os service packs e hot fixes dos dois servidores devem ser os mesmos.
  - Os dois servidores devem residir na mesma floresta do Active Directory e ser integrantes do mesmo domínio ou de domínios confiáveis.
  - Ambos os servidores devem utilizar a mesma porta.
  - Os dois servidores devem ter as mesmas versões de SQL, service packs e hot fixes instaladas.
  - Os dois servidores devem manter sessões idênticas do SQL Server, isto é, padrão ou nomeada.
  - As letras de unidades que contêm arquivos de bancos de dados devem ser idênticas nos dois servidores.
  - O caminho completo do banco de dados padrão do sistema de cada sessão deve ser idêntico nos dois servidores.
- Se estiver instalando o SharePoint com o SQL Server Express Edition, você deve ativar o protocolo TCP/IP da sessão SQL (por exemplo, OfficeServers) nos servidores mestre e de réplica.
- Verifique se a porta definida nas propriedades TCP/IP de configuração da rede, das sessões de SQL, foi atribuída estaticamente e se é idêntica nos servidores mestre e de réplica.
- Nenhum servidor participante pode ser controlador de domínios ou servidor DNS.
- Os servidores mestre e de réplica devem residir na mesma floresta do Active Directory.

Conta de logon de HA do SharePoint

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, será necessário usar uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.
- Se a conta não possuir permissões de Administrador incorporadas em todas as sessões do SQL Server, adicione as permissões adequadas.

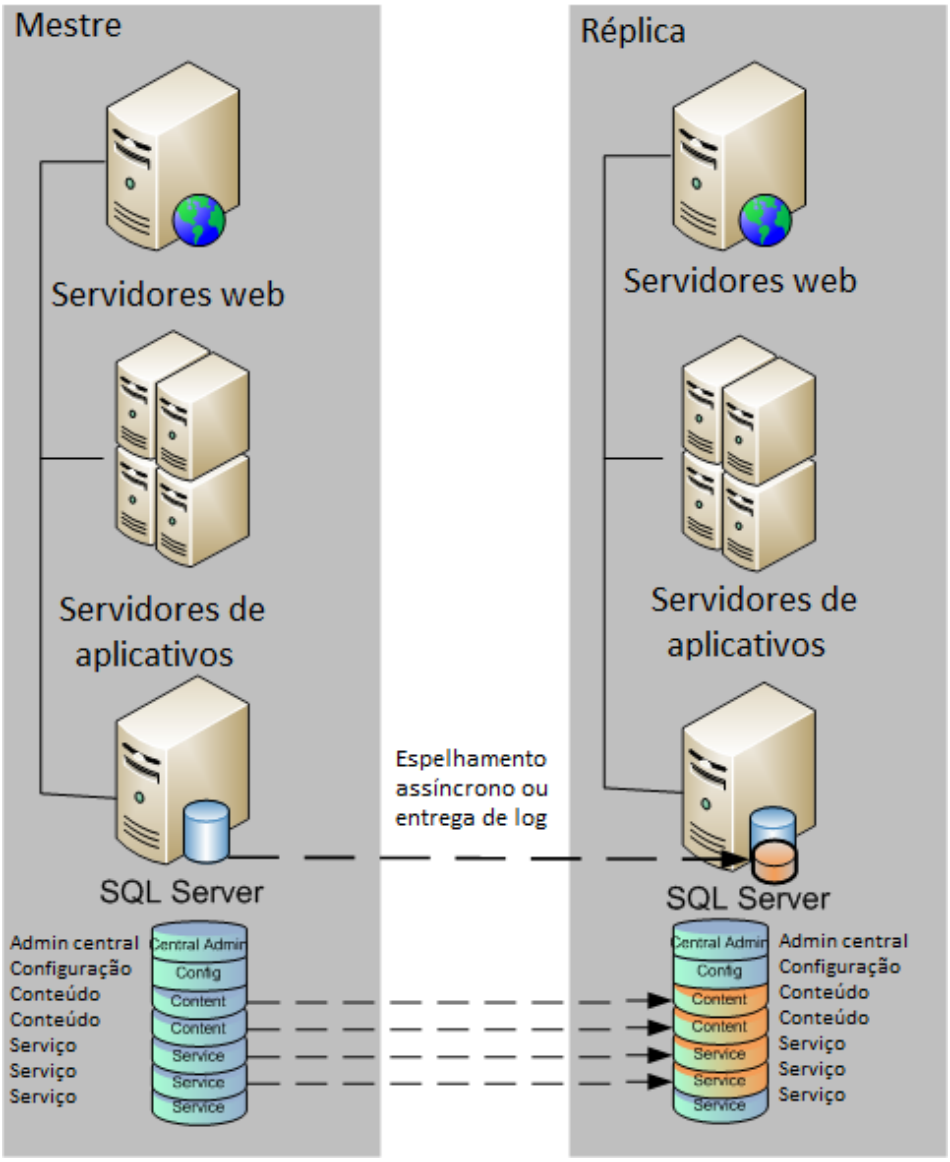
  Observações:

  - Você não deve usar uma conta de Serviço de rede. Isso pode impedir o funcionamento adequado dos serviços após uma alternância.
  - Se a política de segurança de sua empresa exige permissões mais granulares que as descritas, entre em contato com o suporte técnico para receber instruções detalhadas. Para servidores em um grupo de trabalho, mantenha o usuário de logon como sistema local.

Preparar manualmente a réplica para implantação autônoma

Os servidores SharePoint armazenam dados de **configuração** e **conteúdo**. Para proteger ambos os tipos de dados, realize os procedimentos de configuração do servidor de réplica antes de executar qualquer cenário de alta disponibilidade em uma implantação autônoma de um SharePoint Server. O procedimento garante que a réplica seja configurada de maneira idêntica ao mestre.

As implantações autônomas não são redimensionáveis e não podem unir-se a farms do SharePoint. O servidor de réplica é totalmente independente do mestre. O CA ARCserve RHA sincroniza e replica automaticamente o banco de dados de conteúdo no mestre. É preciso manter e personalizar o banco de dados de conteúdo de configuração e administração na réplica, para que seja idêntico ao do mestre antes da execução de um cenário de alta disponibilidade.



Observação: os bancos de dados de conteúdo de configuração e administração não são exibidos na detecção automática ao criar cenários de alta disponibilidade para implantações autônomas do SharePoint Server. Somente os bancos de dados de aplicativos existentes da web podem ser detectados e replicados em cenários de recuperação garantida.

Próximas etapas

Use o assistente de configuração de produtos do SharePoint para preparar a réplica (na página 44)

Use o assistente de configuração de produtos do SharePoint para preparar a réplica

O procedimento a seguir é o método recomendado para configurar o servidor de réplica em implantações autônomas do SharePoint Server. O assistente de configuração de produtos do SharePoint configura os serviços e aplicativos de serviço no servidor de réplica e cria um aplicativo web padrão na porta 80. Antes de iniciar, vá até o Microsoft TechNet para ler as informações sobre como alterar a porta do site de administração. Também é preciso obter as seguintes informações:

- O mapeamento do acesso alternativo e a porta do site administrativo do servidor mestre
- Os nomes de exibição, cabeçalhos e portas para todos os aplicativos web criados no servidor mestre
- Os nomes dos bancos de dados de conteúdo para todos os aplicativos web criados no servidor mestre

Observação: Não execute o procedimento "desconectar do farm"para reconfigurar os servidores do SharePoint configurados automaticamente como réplicas para uso nos novos cenários do CA ARCserve RHA. Desconectar uma réplica configurada automaticamente pode fazer também com que o servidor mestre do cenário antigo se desconecte do farm. Em vez disso, exclua a chave de registro a seguir:

- Para SharePoint Server 2007:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\12.0\Secure\ConfigDB
- Para SharePoint Server 2010:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\14.0\Secure\ConfigDB

Após excluir a chave de registro, é possível executar com segurança o procedimento de desconexão do farm usando o assistente de configuração.

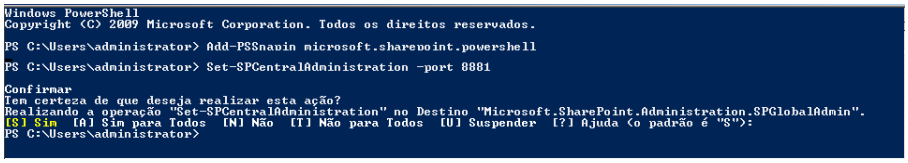
Para usar o assistente de configuração de produtos do SharePoint para preparar a réplica

1. No servidor de réplica, inicie o assistente de configuração de produtos do SharePoint pelo menu Iniciar do Windows.
2. Preencha as telas do assistente. Após a configuração, use a ferramenta PowerShell ou STSADM para alterar a porta do site administrativo na réplica para fazer correspondência com a do mestre.

   Para o PowerShell, forneça o seguinte:

```
set-SPCentralAdministration -Port <PortNumber>
```

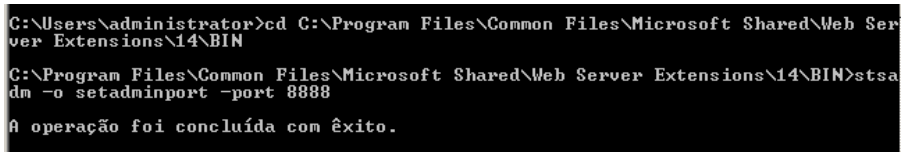
Quando for solicitado a confirmar a ação, digite Y para uma resposta afirmativa.



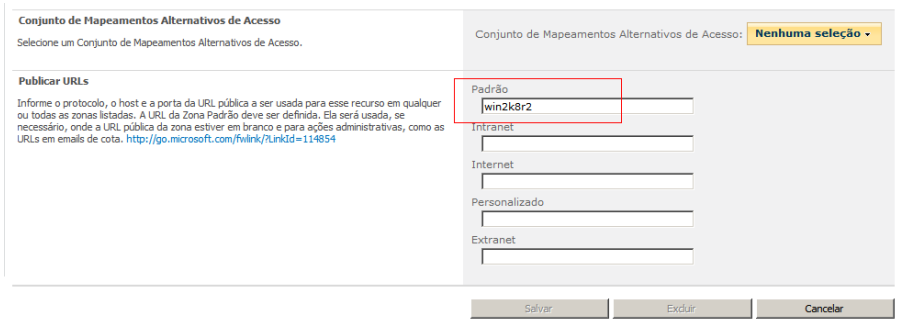
Para o STSADM, forneça o seguinte:

```
stsadm -o setadminport -port <PortNumber>
```

A interface de linha de comando retorna a mensagem Operação concluída com êxito.



3. Inicie a Administração Central do SharePoint 2010 na réplica. Clique em Configurar mapeamentos alternativos de acesso e, em seguida, clique em Editar URLs Públicas. Altere o URL público na réplica para fazer correspondência com a do mestre.



4. Crie aplicativos web na réplica usando os mesmos nomes de exibição, cabeçalhos e portas que os do mestre.

a. Na Administração Central do SharePoint 2010, clique em Gerenciar Aplicativos Web.

b. Clique em Novo.

c. Digite os mesmos nomes de exibição, cabeçalhos e portas usados no servidor mestre para criar aplicativos web.

d. Clique em Gerenciar Bancos de Dados de Conteúdo.

e. Clique em Adicionar um banco de dados de conteúdo.

f. Digite o mesmo nome de banco de dados para cada banco de dados de conteúdo usado no servidor mestre.

5. Crie e execute seus cenários de alta disponibilidade para proteger a implantação autônoma.

Próximas etapas:

- Criar um cenário do SharePoint Server para implantações autônomas
- Crie um cenário do SharePoint Server para implantações de farm (All in One)
- Criar vários cenários para implantações (distribuídas) de farm
- Como executar um cenário ou um grupo

Preparar manualmente a réplica para implantação autônoma

Antes de preparar manualmente a réplica para implantação autônoma, colete as informações a seguir e leia todas as etapas antes de prosseguir:

- Os nomes do banco de dados de configuração do SharePoint Server e do banco de dados de administração central no servidor mestre
- Os nomes de exibição, as portas, os cabeçalhos, o mapeamento do acesso alternativo e os nomes do banco de dados de conteúdo para todos os aplicativos web criados no servidor mestre
- (Para implantações autônomas do SharePoint Server 2007) O nome do provedor de serviços compartilhados no mestre

Também é preciso exibir os seguintes documentos do Microsoft TechNet:

- Psconfig command-line reference (SharePoint Server 2010) (cc263093)
- Command-line reference for the SharePoint Products and Technologies Configuration Wizard (Office SharePoint Server) (para SharePoint Server 2007)
- STSADM.exe command line reference

Importante: O CA ARCserve RHA altera a configuração de uma verificação de loopback da Microsoft para garantir cenários de alta disponibilidade bem-sucedidos nas implantações autônomas do SharePoint. Para obter mais informações, consulte as seguintes informações de suporte da Microsoft.

- http://support.microsoft.com/kb/887993
- http://support.microsoft.com/kb/926642

Para preparar manualmente a réplica para implantação autônoma

1. Colete as informações listadas.
2. Leia os documentos do Microsoft TechNet.

   Observação: o valor dos parâmetros abaixo devem ser idênticos aos do mestre: sp_cfgDB, CenAdmContDB, CentralAdminPort.
3. Abra uma sessão de linha de comando e digite os seguintes comandos.

```
psconfig.exe -cmd configdb -create -server hostname\inst -database sp_cfgDB -
admincontentdatabase CenAdmContDB
psconfig.exe -cmd installfeatures
psconfig.exe -cmd secureresources
psconfig.exe -cmd services -install
psconfig.exe -cmd services -provision (válido apenas para SP2010)
psconfig.exe -cmd adminvs -provision -port centralAdminPort
```

4. Criar aplicativos web na réplica pelo site administrativo central ou pela ferramenta STSADM para que todos os nomes de exibição, cabeçalhos, mapeamento de acesso alternativo, nomes de banco de dados de conteúdo e portas sejam idênticos aos do mestre. Use o nome de host do mestre com a porta como URL de balanceamento de carga ao criar aplicativos web na réplica. Você não precisa criar conjuntos de sites, pois subsites e conjuntos de sites são armazenados no banco de dados de conteúdo, o qual é replicado em cenários do CA ARCserve RHA.
5. Inicie os serviços e crie um provedor de serviços compartilhados (SharePoint Server 2007) ou crie os aplicativos de serviço na réplica para que sejam idênticos aos do mestre usando o site administrativo central.

   Importante: Não use o assistente de configuração de produtos do SharePoint para configurar a réplica antes de executar um cenário de alta disponibilidade.

Replicação e alta disponibilidade do vCenter Server

Replicação do vCenter Server

Esta seção descreve os requisitos para execução do CA ARCserve RHA no vCenter Server.

Configuração de replicação do vCenter

Para implementar a replicação no vCenter Server, são necessárias as seguintes configurações:

- Uma sessão do vCenter Server instalada no mestre.
- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

Para usar a solução de replicação com a opção de **Recuperação garantida** para vCenter Server, são necessárias as seguintes configurações:

- A mesma versão do vCenter Server instalada nos servidores mestre e de réplica.
- O vCenter Server instalado com as mesmas credenciais de logon nos servidores mestre e de réplica.

Conta de logon da replicação do vCenter

A conta de logon do serviço do mecanismo do CA ARCserve RHA deve atender a todas estas condições:

- Para servidores independentes (isto é, não agrupados), use o padrão do sistema local.
- Para nós de agrupamento, use a conta de serviço de um administrador local em todos os nós agrupados.

Alta disponibilidade para vCenter Server

Esta seção descreve os requisitos para execução do CA ARCserve HA para vCenter Server.

Configuração de alta disponibilidade do vCenter Server

Para implementar procedimentos de alta disponibilidade para vCenter Server, você precisa das seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Os dois servidores devem ter as mesmas versões de SQL, service packs e hot fixes instaladas.
- (No ambiente do diretório ativo) os servidores mestre e de réplica devem residir na mesma floresta do diretório ativo e ser integrantes do mesmo domínio ou de domínios confiáveis.
- Atribuir estaticamente todos os endereços IP (não há suporte para endereços IP atribuídos a DHCP no servidor mestre ou de réplica).
- Nenhum servidor participante pode ser controlador de domínios ou servidor DNS.
- Se o Servidor de banco de dados estiver instalado localmente ou remotamente no mestre, configure a réplica para se conectar ao mesmo Servidor de banco de dados.
- Se o Servidor de licenças estiver instalado localmente no mestre, instale outra instância do Servidor de licenças na réplica e configure a réplica para se conectar a ele.
- Se o Servidor de licenças estiver instalado remotamente no mestre, configure a réplica para se conectar a essa instância.

Conta de logon de alta disponibilidade do vCenter

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, use uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.
- Para servidores em um grupo de trabalho, use a conta de sistema local.

Replicação e alta disponibilidade do Microsoft Dynamics CRM

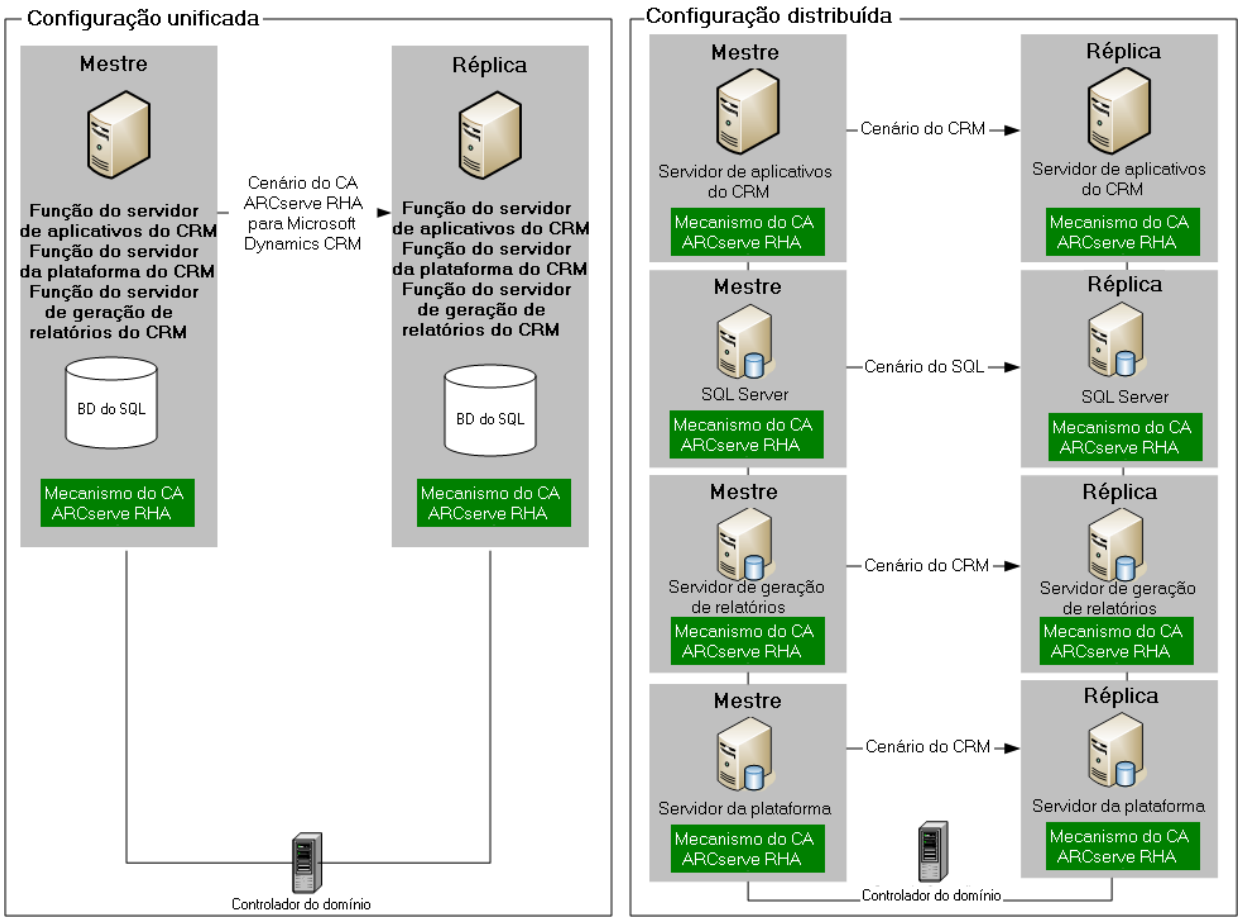
Configuração de replicação e alta disponibilidade do Dynamics CRM

O Microsoft Dynamics CRM é composto de várias funções de servidor que foram combinadas em dois grupos de função de servidor:

- Grupo de função de servidor do aplicativo — este grupo contém os serviços principais do CRM, o front-end da web e a Ajuda.
- Grupo de função de servidor da plataforma — este grupo contém o serviço de processamento assíncrono, o serviço de detecção e o serviço de relatórios.

Os grupos de função de servidor usam o serviço de relatórios do SQL, o qual pode ser instalado em um computador separado. Podem-se instalar os grupos de função de servidor na mesma máquina ou em computadores diferentes.

O CA ARCserve RHA para Microsoft Dynamics CRM pode ser configurado de duas maneiras:



Configuração tudo em um

Todas as funções do grupo de servidores estão em execução na mesma máquina (servidor mestre). Para a opção de configuração tudo em um, é necessário:

- Dois servidores Windows (mestre e réplica) configurados de maneira idêntica. Ao instalar o servidor de réplica, escolha a opção Connect to an existing deployment. Novamente, quando o Dynamics CRM for configurado, é necessário escolher a opção Connect to an existing deployment e, em seguida, fornecer a instância do banco de dados do SQL Server do servidor mestre como o nome do computador que esteja executando o SQL Server a ser usado com a implantação.

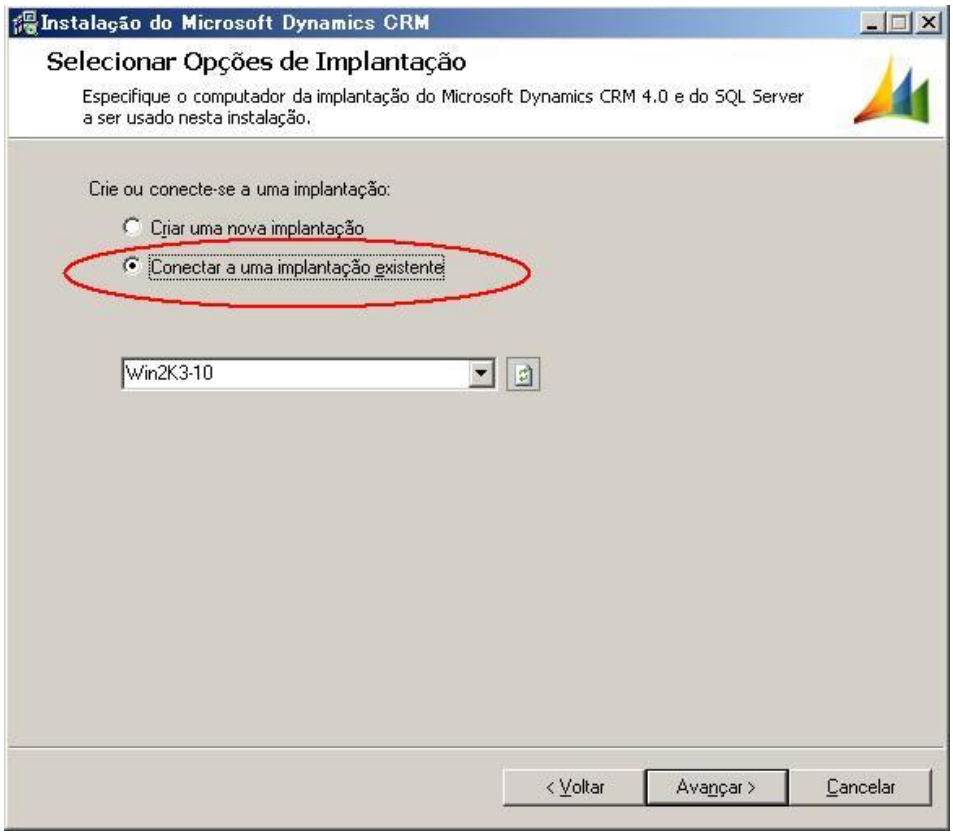
Observação: caso funções de servidor estejam em execução em um único computador, este servidor não pode ser um controlador de domínio, a menos que também esteja executando o Microsoft Windows Small Business Server 2003 Premium Edition R2.

Configuração distribuída

As funções do grupo de servidores estão em execução em máquinas diferentes (vários servidores mestre). Em uma configuração distribuída, é necessário:

- Pelo menos dois servidores Windows (mestre e de réplica) que atuem como servidor de aplicativos do Microsoft Dynamics CRM, servidor da plataforma ou servidor de relatórios. O aplicativo, a plataforma e as funções do servidor de relatórios podem ser assumidas por máquinas individuais ou executadas no mesmo computador. Você pode adicionar servidores conforme necessário. Cada servidor na implantação está protegido por seu próprio cenário do CRM do CA ARCserve RHA, portanto, para cada servidor do Dynamics CRM adicionado, é necessário adicionar também um servidor de réplica configurado de maneira idêntica. Ao instalar o servidor de réplica, escolha a opção Connect to an existing deployment e, em seguida, forneça a instância do banco de dados do SQL Server do servidor mestre como o nome do computador que esteja executando o SQL Server a ser usado com a implantação.
- Dois servidores SQL — um mestre e uma réplica. Esta máquina é protegida separadamente em um cenário de back-end do SQL. Para obter mais informações, consulte o *Guia de Operações para Microsoft SQL Server* do CA ARCserve RHA.

Observação: certifique-se de que o SQL Server Reporting Services e o IIS estejam instalados, antes de instalar o Microsoft Dynamics CRM.



As seguintes regras se aplicam:

- Instale o mecanismo em todos os servidores participantes nos cenários do CA ARCserve RHA.
- Os dois servidores Windows devem estar executando o Windows Server 2003 ou 2008 com o mesmo nível de service packs e hot fixes instalado.
- O servidor a ser protegido não é um controlador de domínios ou um servidor DNS.

Se você estiver executando o SQL 2005 em uma configuração distribuída:

- Certifique-se de que instalou uma sessão do SQL nos dois servidores, o mestre e de réplica.
- Certifique-se de que os dois servidores tenham a mesma versão do SQL, service packs e hot fixes instalados.
- Certifique-se de que os dois servidores mantenham sessões idênticas do SQL Server, ou seja, "padrão" ou "nomeada".
- Verifique se os dois servidores residem na mesma floresta do Active Directory e se são integrantes do mesmo domínio ou de domínios confiáveis.
- Certifique-se de que as letras de unidades que contêm arquivos de bancos de dados sejam idênticas nos dois servidores.
- Certifique-se de que o caminho completo do banco de dados padrão do sistema de cada sessão seja idêntico nos dois servidores.
- Verifique se a porta definida nas propriedades TCP/IP de configuração da rede, das sessões do SQL, foi atribuída estaticamente e se é idêntica nos dois servidores.

Configuração do UNIX/Linux

Em servidores AIX, o nome do host é sempre definido para ser FQDN. Durante a recuperação do FQDN, somente o DNS tem suporte. NIS ou NIS + Naming Service não tem suporte.

Se o redirecionamento de DNS for usado, defina a ordem de pesquisa para classificar associações e hosts no /etc/host.conf.

Um pacote de associações é necessário para o redirecionamento de DNS:

Sistema operacional	Nome do pacote
Linux	bind-utils-*
Solaris	SUNWbind
AIX	bos.rte.bind_cmds

Para Oracle nos sistemas UNIX/Linux, apenas a opção de armazenamento do sistema de arquivos para instância de banco de dados de datafiles é suportada.

Alta disponibilidade de sistema completo

A alta disponibilidade de sistema completo pode ser configurada como segue:

Servidor mestre

Este servidor pode ser qualquer servidor Windows compatível com o mecanismo. O mestre pode ser um servidor virtual ou físico.

Servidor de réplica

Os seguintes ambientes virtualizados são suportados como o servidor de réplica em cenários do tipo Sistema completo:

- Microsoft Hyper-V
- Citrix XenServer (Xen)
- ESX
- vCenter Server
- Amazon EC2

Observação: para o Hyper-V 1.0, verifique se todos os patches estão instalados, principalmente o KB950050. Para obter mais informações, visite o site da Microsoft. Não use o caminho de instalação padrão ao criar máquinas virtuais do Hyper-V. O CA ARCserve RHA não pode acessar o caminho de instalação da máquina virtual padrão durante a detecção automática. Crie uma pasta, como C:\VM\ no mestre e na réplica. Durante a criação do cenário de alta disponibilidade de sistema completo, especifique a pasta na tela Configurações de volume.

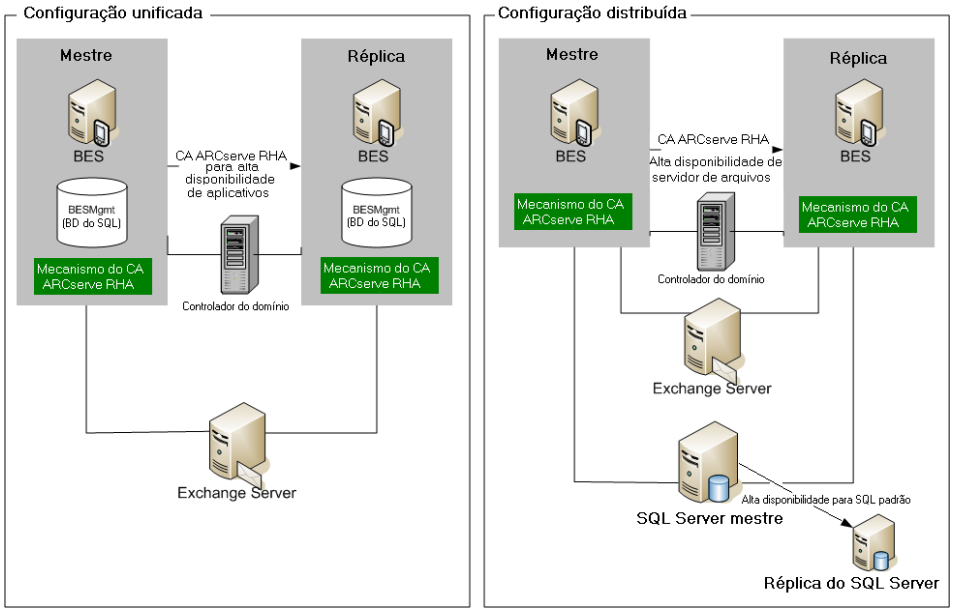
Configurar o Blackberry para o CA ARCserve RHA

Como bem sabe a maioria dos administradores do BlackBerry, as informações de configuração referentes ao BES estão quase que totalmente armazenadas no banco de dados de configuração. Essas informações são essenciais para a operação adequada do BES e também são usadas pelo CA ARCserve RHA para uma alternância bem-sucedida. O banco de dados de configuração poderia ser instalado na mesma máquina que o BES ou em uma máquina diferente, dependendo da necessidade do seu ambiente.

A instalação local ou no mesmo computador cria uma dependência entre o SQL e o BES, estabelecendo uma plataforma vinculada e, com relação à alta disponibilidade, gerenciada junto do CA ARCserve RHA para Aplicativos. Por esse motivo, referimo-nos a essa solução como configuração All in One (Tudo em um).

Se o banco de dados do SQL estiver instalado em um computador diferente (configuração distribuída), você poderá combinar vários cenários de alta disponibilidade para decidir o nível de proteção a ser implementada:

- **Configuração Front-End**--Crie cenários de alta disponibilidade para o servidor de arquivos modificados para usar o script de alta disponibilidade para BlackBerry em ambientes nos quais o banco de dados do SQL já é protegido.
- **Configuração Back-End**--Crie cenários padrão de alta disponibilidade para SQL Server para proteger o servidor SQL separadamente do BES. Para obter mais informações, consulte o Guia de Operações para Microsoft SQL Server do CA ARCserve RHA.



Em um ambiente com dois servidores de produção do BES e um servidor SQL separado, você deve criar três cenários de alta disponibilidade para proteger os seis servidores participantes dos cenários.

Informações adicionais sobre instalação e configuração do CA ARCserve RHA para Blackberry

Proteger seu ambiente Blackberry Enterprise Server com o CA ARCserve RHA requer uma configuração específica e a definição de etapas. Instale o BES nos servidores mestre e de réplica, configure os servidores para alta disponibilidade e, em seguida, conecte o banco de dados ao cenário.

O procedimento completo de instalação e configuração está descrito no *Guia de Operações para BlackBerry Enterprise Server do CA ARCserve RHA* para Windows.

Alta disponibilidade do serviço de controle

Esta seção descreve os requisitos para executar a solução de alta disponibilidade para o serviço de controle do CA ARCserve RHA.

Importante: A solução de alta disponibilidade para o serviço de controle é aplicável somente do CA ARCserve RHA r12.5 e posterior.

Configuração de alta disponibilidade do serviço de controle

Para implementar os procedimentos de alta disponibilidade para o serviço de controle do CA ARCserve RHA, é necessário ter as seguintes configurações:

- Dois servidores executando uma versão do Windows Server com suporte e o mesmo nível de service packs e hot fixes instalado.

  Observação: para obter uma lista completa de aplicativos e sistemas operacionais com suporte, consulte as Notas da Versão do CA ARCserve RHA.

- Uma sessão de um serviço de controle instalada em cada servidor. Ambas as sessões devem ter a mesma versão do serviço de controle.
- Os service packs e hot fixes dos dois servidores devem ser idênticos.
- (No ambiente do diretório ativo) os servidores mestre e de réplica devem residir na mesma floresta do diretório ativo e ser integrantes do mesmo domínio ou de domínios confiáveis.
- Ambos os servidores devem utilizar a mesma porta.
- Nenhum servidor participante pode ser controlador de domínios ou servidor DNS.

Conta de logon de alta disponibilidade do serviço de controle

A conta de logon do serviço mecanismo do CA ARCserve HA deve atender a todas estas condições:

- Deve ser integrante do grupo de administradores do domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, use uma conta que o seja.
- Deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente.
- Para servidores em um grupo de trabalho, use a conta de sistema local.

Observação: se a política de segurança de sua empresa exige permissões mais granulares que as descritas, entre em contato com o suporte técnico para receber instruções detalhadas.

Apêndice A: Instalar, atualizar e desinstalar o CA ARCserve RHA

Esta seção apresenta instruções sobre o processo de instalação do CA ARCserve RHA e descreve como executar uma atualização.

Esta seção contém os seguintes tópicos:

Registrar o Windows Installer

O serviço Windows Installer deve estar corretamente instalado e registrado para que o CA ARCserve RHA possa ser instalado. Se este serviço for interrompido ou danificado, o seguinte erro ocorre ao instalar ou desinstalar alguns aplicativos:

Erro 1720 ou 1722 do Windows Installer

Há duas formas de evitar este erro:

- Registre novamente a versão atual do serviço Windows Installer
- Faça download da versão mais recente do serviço Windows Installer

Para registrar novamente a versão atual, clique em Iniciar, Executar e digite os seguintes comandos:

```
Msiexec/unregister
```

```
Msiexec/regserver
```

Para instalar a versão mais recente do serviço Windows Installer

1. Vá até o site da Microsoft e faça download da versão mais recente do Windows Installer.
2. Siga as instruções da Microsoft para instalar o serviço de acordo com os requisitos do sistema.
3. Reinicie o computador após a instalação ser concluída.
4. Verifique se o serviço está em execução. Clique em Iniciar, Executar e digite o seguinte comando:

   ```
   services.msc
   ```

   Se você estiver executando o Vista, digite o comando em Iniciar, na caixa de pesquisa.

   A janela Serviços é aberta. Localize o serviço Windows Installer e verifique se o status está como Iniciado. Altere o tipo de inicialização para Automático, se necessário, e inicie o serviço manualmente, caso ele não esteja em execução.

Depois que o Windows Installer estiver instalado e verificado, pode-se instalar o CA ARCserve RHA.

Instalação inicial do CA ARCserve RHA

Instalar componentes do CA ARCserve RHA pela primeira vez é muito fácil. O pacote de instalação, disponível para download no site do CA ARCserve RHA, contém um arquivo de instalação denominado Setup.exe. O Setup.exe executa um assistente de instalação padrão que orienta a instalação.

- Esta instalação não exige reinicialização nem encerramento do aplicativo.
- A versão necessária do Windows Installer (INSTMSI.EXE) é a 3.0. Salvo indicação em contrário, todos os sistemas operacionais suportados possuem o Windows Installer 3.0 como aplicativo incorporado.

Solicitações padrão facilitam a instalação. A única decisão importante é em quais servidores instalar os diferentes componentes:

- Instale o serviço de controle em um computador utilizado para monitorar e gerenciar todos os cenários.
- Instale o mecanismo nos servidores mestre e de réplica.
- O usuário que instalar os componentes do CA ARCserve RHA deverá ter privilégios administrativos locais ou ser um integrante do grupo local de administradores.

O diretório padrão da instalação é:
INSTALLDIR\Program Files\CA\ARCServe RHA\component_names.

- Durante o processo de instalação, você é solicitado a inserir a conta em que o serviço do CA ARCserve RHA será executado.
- Se você estiver executando cenários de alta disponibilidade (HA), a conta em que o serviço do CA ARCserve RHA estiver sendo executado poderá exigir outros privilégios além daqueles atribuídos à conta de sistema local. (Consulte o Guia de Operações do CA ARCserve Replication adequado para obter mais informações.)
- Uma conta de usuário do Windows que executa o serviço de controle do CA ARCserve RHA precisa ter permissão de leitura e gravação no diretório de instalação.
- A conta de logon do serviço para o mecanismo do CA ARCserve RHA exige permissão de leitura e gravação no diretório de instalação.

Fluxo de trabalho da instalação de componentes

A instalação de componentes básicos do CA ARCserve RHA inclui várias etapas simples:

1. Instalação do serviço de controle - instale o serviço de controle em um servidor autônomo da Microsoft, use o arquivo **Setup.exe**, selecione a opção **serviço de controle do CA ARCserve RHA** e siga as instruções do assistente.
2. Instalação do gerenciador - abra a página Visão geral do CA ARCserve RHA. Ao clicar no link **Gerenciamento de cenários** nesta página, o sistema instalará automaticamente o gerenciador do CA ARCserve RHA no computador local.
3. Instalação de mecanismos – abra o gerenciador e crie um novo cenário, usando o Assistente de criação de cenários. Durante a criação do cenário, o sistema permite a instalação do Mecanismo nos hosts Mestre e de Réplica que participam do cenário. Também é possível instalar um mecanismo localmente, usando o arquivo **Setup.exe**, ou instalar vários mecanismos de uma vez, usando o programa de instalação remota.

Instalar o CA ARCserve RHA para Microsoft Failover Cluster

Em cada nó do ambiente de agrupamento, execute o plug-in do MSFC do CA ARCserve RHA denominado CAARCserveRHAforMSFC.exe ou CAARCserveRHAforMSFC64.exe (versão de 64 bits) para iniciar o assistente do InstallShield, que o guiará pelo processo de instalação do Recurso de disco do CA ARCserve RHA para Microsoft Failover Cluster e o Snap-In do MMC para Gerenciador de agrupamento de disco do CA ARCserve RHA.

Preencha as telas do assistente para instalar o CA ARCserve RHA para Microsoft Failover Cluster. Você pode escolher a instalação Concluído ou Personalizado.

- **Concluído** -- instala todos os componentes do programa
- **Personalizada** -- instala os componentes que você especificar

Observação: após a instalação, é preciso reiniciar o mecanismo do CA ARCserve RHA antes de criar um recurso de disco. O Microsoft .NET Framework 3.5 é obrigatório. Se o software não o detectar, você será solicitado a instalá-lo e repetir a instalação.

Durante a instalação, os processos necessários são adicionados ao Firewall do Windows, como exceções. Se estiver usando outro produto de firewall ou configurou um manualmente, é necessário lembra-se de adicionar os processos do CA ARCserve RHA para Microsoft Failover Cluster como exceções para garantir a comunicação adequada entre o MMC e o mecanismo do CA ARCserve RHA.

Atualização da instalação

Embora o CA ARCserve RHA seja diferente da versão anterior em muitos aspectos, não há diferença importante entre uma nova instalação e a atualização da versão existente. O sistema detecta automaticamente componentes anteriores e o assistente de MSI executa todas as tarefas necessárias para atualizar o aplicativo. Muitos componentes da versão anterior podem permanecer na rede e você pode importar cenários existentes e reutilizá-los no gerenciador do CA ARCserve RHA.

Importante: O cenário Sistema completo deve ser executado novamente ao menos uma vez após a atualização para r16.0 SP2 a partir de uma release anterior.

Observação: os cenários criados na versão anterior foram salvos por padrão em *INSTALLDIR:\Program Files\CA/ARCserve RHA\ws_scenarios*. Para obter mais informações sobre o processo de importação, consulte o *Guia de Administração do CA ARCserve RHA*.

Para uma atualização bem-sucedida, o único componente que você precisa remover é o mecanismo anterior do CA ARCserve RHA. Por isso, é necessário desinstalar o CA ARCserve RHA de cada servidor mestre e de réplica. Use o arquivo Setup.exe para automatizar esse procedimento ou faça-o manualmente antes de iniciar a nova instalação.

Observação: se estiver tentando instalar o serviço de controle em um computador com a interface de usuário de uma versão anterior, esta mensagem será exibida:

Foi detectada uma versão anterior do CA ARCserve RHA. Não é necessário removê-la para instalar a nova versão.

Clique em **OK** e continue a instalação.

Para remover o Mecanismo anterior usando o arquivo setup.exe:

1. Clique duas vezes no arquivo de instalação **Setup.exe**. O assistente de instalação do CA ARCserve RHA é exibido.
2. Clique na opção **Instalar**. A página **Instalar componentes** é apresentada.
3. Clique na opção **Instalar mecanismo do CA ARCserve RHA**. Clique na opção **Instalar mecanismo do CA ARCserve RHA**.

   A caixa de diálogo **Escolher idioma de instalação** é exibida.

4. Selecione, na lista suspensa, o idioma do assistente de instalação que preferir e clique em **OK**.

   Uma barra de andamento é apresentada.

5. Após a conclusão do processo inicial, a página **Bem-vindo** é apresentada.
6. Clique em **Avançar**. O sistema detecta se existe um mecanismo anterior no servidor e a página **Informações sobre a versão anterior** é apresentada.
7. Para remover automaticamente o mecanismo anterior, clique em **Avançar**. Uma barra de andamento é apresentada.
8. Após a conclusão do processo de remoção, a página **Contrato de Licença** aparece.
9. Siga as instruções do assistente até concluir a instalação, conforme descrito na seção Instalando o mecanismo do CA ARCserve RHA.

Observação: todos os marcadores e pontos de retrocesso existentes são perdidos após a atualização.

Atualização em fases

Esta release do CA ARCserve RHA é compatível com a versão anterior e, portanto, pode-se atualizá-la ao longo do tempo.

Para executar o CA ARCserve RHA em um ambiente misto, verifique o seguinte:

- Primeiro, atualize o serviço de controle.
- Caso não esteja planejando atualizar os servidores mestre e de réplica ao mesmo tempo, certifique-se de atualizar o mestre antes da réplica. Não há suporte para replicação de cenário de retorno até que os dois servidores estejam atualizados.
- Para cenários de alta disponibilidade, devem-se atualizar os servidores mestre e de réplica ao mesmo tempo.
- Não é possível criar os cenários do novo servidor de arquivos ou do aplicativo quando uma versão mais antiga do mecanismo estiver em execução, mas podem-se criar cenários novos de CD.

Aplicativo proxy XONET

O aplicativo proxy XONET é um serviço com base no TCP/IP que permite versões anteriores e atuais dos mecanismos do CA ARCserve RHA existirem na mesma porta de rede. Use-o quando desejar atualizar gradualmente uma grande base de instalação de distribuição de conteúdo. Consulte o tópico, Desinstalar aplicativos v4 e proxy, quando estiver pronto para remover a versão anterior.

A configuração do XONET é feita automaticamente durante o processo de atualização. Ao instalar a atualização em outra porta, o XONET monitora a porta 25000 e analisa as conexões de entrada. Todas as conexões v4 são roteadas para a porta 24000 (padrão) e todas as conexões da versão atual para a porta 26000 (padrão).

Para obter mais informações, consulte o tópico, Aprimoramentos do programa de instalação.

Observação: o proxy XONET oferece suporte somente a plataformas Windows.

Pacote do InstallShield

O pacote do InstallShield para CA ARCserve RHA foi aperfeiçoado com uma nova opção Preserve v4, a fim de oferecer suporte a um plano de atualização em fases. Ative esta opção para manter instalações anteriores ao instalar a versão atual do CA ARCserve RHA. O programa de instalação modifica a configuração da porta existente, armazenada no arquivo ws_rep.cfg da v4 para 24000 e instala um novo arquivo ws_rep.cfg com a configuração de porta 26000.

O programa de instalação remota também oferece suporte a instalações que preservem a v4. Durante a verificação do cenário, o programa de instalação remota detecta as versões de todos os produtos do CA ARCserve RHA instalados na máquina de destino. Ao detectar a v4, a caixa de diálogo Configurações de instalação apresenta uma opção adicional, Desinstalar o mecanismo da versão 4 antes da atualização. Esta opção é ativada por padrão. Caso deseje manter a v4, desmarque a caixa de seleção para exibir campos adicionais. Os cenários da v4 são importados e convertidos automaticamente.

Importante: se você instalar o proxy XONET em um cluster da Microsoft, deve-se também instalar a hotfix T5LT025 ou ele não funcionará. Para obter a correção, entre em contato com o suporte para solicitá-la.

Porta da versão 4

Este é o número da porta para a qual o mecanismo da v4 será movido. O valor padrão, 24000, não deve ser alterado.

Porta Proxy

Este é o número da porta na qual o aplicativo proxy XONET efetuará a detecção. O valor padrão, 25000, não deve ser alterado.

Número de porta

Este é o número da porta na qual o mecanismo da versão atual efetua a detecção. O valor padrão, 26000, não deve ser alterado.

O programa de instalação também executa o seguinte:

- Migra todos os usuários de segurança delegados para os grupos de segurança correspondentes para a versão atual;
- Importa e converte na versão atual os cenários criados na versão anterior;
- Permite desinstalar aplicativos proxy e v4 conforme sua conveniência.

Observação: a instalação do proxy é feita automaticamente durante a atualização; não existe nenhum executável separado.

Desinstalar aplicativos v4 e proxy

É possível desinstalar aplicativos v4 e proxy manualmente e em cada servidor.

Para desinstalar aplicativos v4 e proxy

1. Interrompa o serviço proxy do XONET por meio do mini-aplicativo Services.
2. Execute o serviço proxy do XONET com a opção -uninstall para removê-lo.
3. Se desejar, remova o aplicativo proxy XONET do disco.
4. Desinstale o WANsync v4 com a opção Adicionar/remover programas no painel de controle do Windows.
5. Edite a configuração da porta no arquivo ws_rep.cfg da versão atual para 25000.
6. Reinicie o mecanismo por meio do miniaplicativo de serviços.

Solução de problemas do proxy XONET

Sintoma:

Não é possível acessar o mecanismo a partir da interface de usuário (ele é exibido como desconectado).

Solução:

Faça o seguinte:

1. Verifique se o serviço do mecanismo está ativo e em execução (vá até o miniaplicativo de serviços e verifique o status do mecanismo).
2. Verifique se o serviço proxy está ativo e em execução (vá até o miniaplicativo de serviços e verifique o status do serviço CAXOProxy).
3. Verifique se as portas do mecanismo, para as versões v4 e atual, correlacionam com a configuração das portas do serviço proxy. Configuração das portas padrão do proxy (vá até o miniaplicativo de serviços e clique duas vezes na entrada do serviço proxy. Verifique os parâmetros de Caminho do campo do executável).
   a. A porta proxy principal deve ser 25000.
   b. A porta do proxy da v4 deve ser 24000 (a porta do mecanismo da v4 deve escutar esta porta; verifique o arquivo ws_rep.cfg na v4).
   c. A porta da versão atual do proxy deve ser 26000 (o mecanismo deve escutar esta porta; verifique o arquivo ws_rep.cfg).
4. Verifique se os cenários para a v4 e a versão atual se referem à porta principal do proxy (nas opções Cenário, Mecanismo, a porta do mecanismo deve ser definida com o valor padrão da porta principal do proxy (25000).

Instalar o serviço de controle do CA ARCserve RHA

Esta seção descreve como instalar o serviço de controle do CA ARCserve RHA.

Considerações sobre a instalação do serviço de controle

É preciso instalar um ou dois serviços de controle, dependendo do tipo de procedimento que você deseja executar no serviço de controle:

- Para as operações padrão de replicação e alta disponibilidade do CA ARCserve RHA, é necessário instalar somente um serviço de controle (na página 72). Esse serviço de controle funcionará como o ponto único de controle de todas as operações do CA ARCserve RHA. Se desejar replicar dados do serviço de controle SEM executar alternância entre dois serviços de controle, você também pode instalar apenas um serviço de controle.

  Observação: após concluir a instalação de todos os componentes do CA ARCserve RHA, para replicar dados do serviço de controle, é necessário criar um cenário de serviço de controle da replicação usando o gerenciador.

- Para replicar dados do serviço de controle e alternar funções entre o serviço de controle original e o serviço de controle em espera, é preciso instalar dois serviços de controle (na página 76). Um dos serviços de controle instalado funcionará como o serviço de controle ativo, enquanto os outros funcionarão como o serviço de controle em espera. Para instalar dois serviços de controle, é preciso repetir o processo de instalação duas vezes, já que só é possível instalar um serviço de controle de cada vez.

  Observações:

  - Para aplicar a solução de alta disponibilidade no serviço de controle, é preciso criar um cenário de alta disponibilidade do serviço de controle com o gerenciador, após a conclusão da instalação de todos os componentes do CA ARCserve RHA.
  - Você NÃO precisa de uma licença de alta disponibilidade para aplicar uma solução de alta disponibilidade no serviço de controle. No entanto, é preciso registrar o CA ARCserve RHA antes de criar um cenário para o serviço de controle.
  - Para obter mais informações sobre a criação de cenários de replicação e alta disponibilidade do serviço de controle, consulte o Guia de Administração do *CA ARCserve RHA*.

Instalar um serviço de controle para uma operação padrão

Para instalar o serviço de controle do CA ARCserve RHA:

1. Clique duas vezes no arquivo de instalação **Setup.exe**. O assistente de instalação do CA ARCserve RHA é exibido.
2. Clique na opção **Instalar**. A página **Instalar componentes** é apresentada.

3. Clique na opção **Instalar serviço de controle do CA ARCserve RHA**. A caixa de diálogo **Escolher idioma de instalação** é exibida.

4. Selecione, na lista suspensa, o idioma do assistente de instalação que preferir e clique em **OK**.

   Uma barra de andamento é apresentada. Após a conclusão do processo inicial, a página **Bem-vindo** é apresentada.

5. Clique em **Avançar**. A página **Contrato de licença** é apresentada.

6. Marque a caixa de seleção **Eu aceito** e clique em **Avançar**. A página **Informações do cliente** é exibida.

7. Verifique se os detalhes estão corretos nos campos ou altere-os de forma adequada. A seguir, clique em **Avançar**. A página **Pasta de destino** é apresentada.

8. Escolha o local de instalação do serviço de controle, usando o botão **Alterar** ou deixe-o no local padrão. A seguir, clique em **Avançar**.

   Observação: o diretório de instalação padrão é *\Program Files\CA\ARCserve RHA\component_name*. Todos os arquivos executáveis, DLLs e de configuração estão no diretório INSTALLDIR.

   A página **Configuração SSL** é exibida.

9. A página **Configuração SSL** permite usar certificado SSL para proteger a comunicação com o serviço de controle.

   Se em seu ambiente de TI, o software estiver implantado em uma rede local e não houver preocupação em relação à segurança, pode-se desmarcar a caixa de seleção **Usar a configuração SSL.** A comunicação com o Serviço de controle será realizada em HTTP.

   Se desejar usar a configuração SSL, marque a caixa de seleção **Usar Configuração SSL**. Neste caso, a comunicação com o Serviço de controle será realizada em HTTPS. Após selecionar essa opção, é preciso inserir um número de porta na caixa **Porta SSL** e especificar o arquivo de certificados em uma das caixas de tipo de certificado disponíveis.

Observações:

- Quando é selecionada a opção **Configuração SSL**, o número padrão da **Porta SSL** é **443**. Porém, se esse número de porta estiver em uso no ambiente de TI, use outra porta.
- Se você selecionou a opção **Configuração SSL,** ao abrir a página Visão geral será necessário usar o nome do host do computador do serviço de controle (em vez do endereço IP). Insira o nome do host e o número da porta do Serviço de controle, conforme abaixo:
  https://nome_host:núm_porta/página_inicial.aspx
- Os certificados .CER e .PEX são arquivos de segurança na Internet fornecidos por autoridades de certificação de terceiros. Esses certificados são instalados em um servidor Web para autenticar a validade de determinado site hospedado no servidor. Eles são representados por um ícone de cadeado próximo à borda de uma janela do navegador ao acessar um site seguro (que começam com "https://"). Depois de especificar o caminho e o nome de um certificado .CER de .PEX na página Configuração SSL, o assistente do InstallShield do serviço de controle do CA ARCserve RHA instala o certificado e adiciona as informações meta do certificado SSL no servidor web. Essas informações meta são mantidas pela API do HTTP em um armazenamento meta e são usadas para localizar certificados durante a troca em sessões HTTPS.
- Se não possuir um certificado SSL autorizado, use o **Certificado auto-assinado**. Após selecionar o botão de opção **Certificado auto-assinado**, ao tentar acessar a página Visão geral de um computador remoto, você precisará instalar o certificado. Para obter mais informações, consulte Instalando certificado SSL auto-assinado (na página 97).

10. Clique em **Avançar**. A página **Informações de logon do serviço** é apresentada.
11. Selecione e insira as informações necessárias. Você pode usar privilégios da conta de sistema local ou fornecer nome e senha de usuário no formulário de Domínio/Nome de usuário.

    Observação: executar o serviço de controle em uma conta de domínio com direitos administrativos em vários computadores permite a implantação remota e conexão ao mecanismo, sem que seja solicitada a autenticação em cada servidor.

12. Clique em **Avançar**. A página **Função do serviço de controle** é exibida.

    Observação: somente se você desejar instalar dois serviços de controle para alternar função (na página 76), marque a caixa de seleção **Allow the Control Service** (Permitir o serviço de controle) e defina se o serviço de controle atualmente instalado assumirá a função do controle de serviço **Ativo** ou **Em espera**.

13. Para uma instalação típica do serviço de controle, clique em **Avançar**. A página **Pronto para instalar o programa** é exibida.

    Observação: clique no botão **Voltar** para retornar às páginas anteriores e alterar a configuração.

14. Clique no botão **Instalar** para instalar o serviço de controle. A página **Instalando o serviço de controle** é exibida.

15. Concluída a instalação, clique em **Avançar**. A próxima página é apresentada.

16. Clique em **Concluir** para fechar o assistente. Agora, o serviço de controle está instalado no local selecionado.

Instalar dois serviços de controle para alternância de serviço de controle

A instalação de dois serviços de controle para alternar função é muito semelhante à instalação padrão. Há somente duas diferenças principais:

- Para instalar dois serviços de controle, é preciso repetir o processo de instalação duas vezes.
- É preciso definir, durante o processo de instalação, se o serviço de controle que você está instalando funcionará como serviço de controle ativo ou como serviço de controle em espera.

Para instalar o serviço de controle para alternância de função:

1. Clique duas vezes no arquivo de instalação **Setup.exe**. O assistente de instalação do CA ARCserve RHA é exibido.
2. Clique na opção **Instalar**. A página **Instalar componentes** é apresentada.
3. Clique na opção **Instalar serviço de controle**. A caixa de diálogo **Escolher idioma de instalação** é exibida.
4. Selecione, na lista suspensa, o idioma do assistente de instalação que preferir e clique em **OK**.

   Uma barra de andamento é apresentada. Após a conclusão do processo inicial, a página **Bem-vindo** é apresentada.
5. Clique em **Avançar**. A página **Contrato de licença** é apresentada.
6. Marque a caixa de seleção **Eu aceito** e clique em **Avançar**. A página **Informações do cliente** é exibida.
7. Verifique se os detalhes estão corretos nos campos ou altere-os de forma adequada. A seguir, clique em **Avançar**. A página **Pasta de destino** é apresentada.
8. Escolha o local de instalação do serviço de controle, usando o botão **Alterar** ou deixe-o no local padrão. A seguir, clique em **Avançar**.

   Observação: o diretório padrão de instalação (INSTALLDIR) é: *Program Files**CA**ARCserveRHA**nome_do_componente*. Todos os arquivos executáveis, DLLs e de configuração estão no diretório INSTALLDIR.

   A página **Configuração SSL** é exibida.
9. A página **Configuração SSL** permite usar certificado SSL para proteger a comunicação com o serviço de controle.
   - Para utilizar a opção Configuração SSL, consulte Instalação de um serviço de controle para uma operação padrão (na página 72).

- Para utilizar o certificado auto-assinado do SSL, consulte Instalando o Certificado auto-assinado do SSL (na página 97).

10. Após selecionar a configuração de comunicação, clique em **Avançar**. A página **Informações de logon do serviço** é apresentada.

    Selecione e insira as informações necessárias. Você pode usar privilégios da conta de sistema local ou fornecer nome e senha de usuário no formulário de Domínio/Nome de usuário.

    Observação: executar o serviço de controle em uma conta de domínio com direitos administrativos em vários computadores permite a implantação remota e conexão ao mecanismo, sem que seja solicitada a autenticação em cada servidor.

11. Clique em **Avançar**. A página **Função do serviço de controle** é exibida.

    Para instalar o serviço de controle para alternar, marque a caixa de seleção **Permitir o serviço de controle**. Depois, defina se o controle de serviço atualmente instalado assumirá a função como **Ativo** ou **Em espera**.

12. Clique em **Avançar**. A página **Pronto para instalar o programa** é exibida.

    Observação: clique no botão **Voltar** para retornar às páginas anteriores e alterar a configuração.

13. Clique no botão **Instalar** para instalar o serviço de controle. A página **Instalando o serviço de controle do CA ARCserve RHA** é exibida, mostrando o progresso da instalação.

14. Concluída a instalação, clique em **Avançar**. A página **Assistente do InstallShield concluído** é exibida.

15. Clique em **Concluir** para fechar o assistente. Agora, o serviço de controle está instalado no local selecionado.

16. Repita o processo de instalação para o segundo serviço de controle (Ativo ou Em espera).

17. Instalar o mecanismo do CA ARCserve RHA (na página 79) nos servidores de destino dos dois serviços de controle.

Instalar o serviço de controle usando a CLI

Você pode instalar o serviço de controle do CA ARCserve RHA usando a interface de linha de comando.

Para instalar o serviço de controle do CA ARCserve RHA usando a CLI

- Abra a CLI e digite o seguinte:

```
CAARCserveRHAManager.exe /S "/v/qn XOLOGIN="[Domain/UserName]"
XOPASSWORD="[Password]" XOLANG="[Language]"
```

Parâmetros

CAARCserveRHAManager.exe

O arquivo de instalação do serviço de controle do CA ARCserve RHA

S, V, QN

Parâmetros de instalação silenciosa

Domain/UserName, Password

Insira as informações necessárias de acordo com a plataforma utilizada e a solução implementada, conforme descrito no capítulo Requisitos de aplicativos e bancos de dados suportados (na página 21). Se você não inserir os detalhes da Conta de logon, o padrão será o Sistema local.

Idioma

Selecione o idioma do CA ARCserve RHA, usando um dos seguintes códigos de idioma:

- "1033" inglês
- "1036" francês
- "1041" japonês
- "2052" chinês (simplificado)
- "1028" chinês (tradicional)
- "1031" alemão
- "1034" espanhol
- "1040" italiano
- "1046" português (Brasil)

Observação: não é possível usar a instalação silenciosa do serviço de controle.

Exemplo: instalar o serviço de controle usando a CLI

```
CAARCserveRHAManager.exe /S "/v/qn XOLOGIN="domain/administrator"
XOPASSWORD="abcd" XOLANG="1033"
```

Como instalar o mecanismo do CA ARCserve RHA

Esta seção descreve como instalar o mecanismo do CA ARCserve RHA.

A seguir veja três formas de instalar o mecanismo do CA ARCserve RHA:

- Usando o arquivo Setup.exe – instale o mecanismo em um host por vez. Este método de instalação detecta automaticamente o Mecanismo da versão anterior e permite removê-lo durante a instalação do novo Mecanismo. As etapas de instalação são semelhantes às da instalação do serviço de controle, conforme descrito em Instalando o serviço de controle do CA ARCserve RHA.
- Usando o Assistente de criação de cenários – instale remotamente o mecanismo nos hosts mestre e de réplica, durante a criação de um novo cenário.
- Usando o Programa de instalação remota – instale remotamente o mecanismo em um ou mais hosts de uma só vez, usando o assistente de instalação remota.

Instalando o mecanismo do CA ARCserve RHA em um Windows Server 2008 R2 Server Core

Antes de instalar o mecanismo do RHA em um Windows 2008 R2 Server Core, registre o arquivo ieproxy.dll e instale o pacote redistribuível do Visual C++ 2005.

Siga estas etapas:

1. Navegue até a pasta %programfiles%\Internet Explorer no Windows Server 2008 R2 (instalação diferente do Server Core).
2. Localize o arquivo ieproxy.dll e copie-o para o seguinte local do Server Core:

   ```
   %systemRoot%\system32
   ```

3. Para fazer o registro, digite o comando a seguir no prompt:

   ```
   regsvr32 %systemRoot%\system32\ieproxy.dll
   ```

4. Instale o pacote redistribuível do Microsoft Visual C++ 2005 (x64). Faça download do pacote redistribuível no site www.microsoft.com.

Instalar o mecanismo com o arquivo de instalação Setup.exe

Para instalar o mecanismo do CA ARCserve RHA usando o arquivo Setup.exe

1. Clique duas vezes no arquivo de instalação **Setup.exe**. O assistente de instalação do CA ARCserve RHA é exibido.
2. Clique na opção **Instalar**. A página **Instalar componentes** é apresentada.
3. Clique na opção **Instalar mecanismo do CA ARCserve RHA**. A caixa de diálogo **Escolher idioma de instalação** é exibida.
4. Selecione, na lista suspensa, o idioma do assistente de instalação que preferir e clique em **OK**.

   Uma barra de andamento é apresentada. Após a conclusão do processo inicial, a página **Bem-vindo** é apresentada.
5. Clique em **Avançar**. A página **Contrato de licença** é apresentada.

   Observação: quando há um mecanismo de uma versão anterior no servidor, a página **Informações sobre a versão anterior** é apresentada com a opção de desinstalar o mecanismo.
6. Na página **Contrato de licença**, marque a caixa de seleção **Eu aceito** e clique em **Avançar**. A página **Pasta de destino** é apresentada.
7. Verifique se os detalhes estão corretos nos campos ou altere-os de forma adequada. A seguir, clique em **Avançar**. A página **Personalizar instalação** é apresentada.

   Observação: quando a opção **Mecanismo** é selecionada, o botão **Espaço** é ativado. Clicar nesse botão permite a visualização do espaço em disco necessário para a instalação do recurso selecionado.

8. Clique em **Avançar**. A página **Informações de logon do serviço** é apresentada.
9. Insira as informações necessárias de acordo com a plataforma utilizada e a solução implementada, conforme descrito no capítulo Requisitos de aplicativos e bancos de dados suportados.
   - Para o Servidor de arquivos use estas diretrizes:
     - Para cenários de replicação – é suficiente usar a conta de sistema local.
     - Para agrupamentos (cenários de replicação) - é necessário executar na mesma conta do serviço de agrupamento ou com permissões equivalentes.
     - Para cenários de alta disponibilidade (incluindo agrupamentos) –
     - É necessário executar em uma conta com os privilégios administrativos de domínio. Se o grupo de administradores do domínio não for integrante dos administradores do grupo local do domínio incorporado, será necessário usar uma conta que o seja.
     - A conta também deve ser integrante do grupo de administradores do computador local. Se o grupo de administradores do domínio não for um integrante, adicione a conta manualmente. Para servidores em um grupo de trabalho, use a Conta de sistema local.
10. Clique em **Avançar**. A página **Pronto para instalar o programa** é exibida.
11. Clique em **Instalar**. A página **Instalando o mecanismo do CA ARCserve RHA** é apresentada.
12. Concluída a instalação, clique em **Avançar**. A página **Assistente do InstallShield concluído** é apresentada.
13. Clique em **Concluir** para terminar a instalação.

Instalar o mecanismo usando o assistente de criação de cenários

Para instalar o mecanismo com o assistente de criação de cenários

1. No menu **Cenário** do gerenciador do CA ARCserve RHA, selecione a opção **Novo**.

   O **Assistente de criação de cenários** é apresentado.

2. Selecione as opções de cenário necessárias, da seguinte forma:

   - Selecione o botão de opção **Criar cenário**.
   - Na lista suspensa **Grupo**, selecione o grupo ao qual deseja atribuir o novo cenário ou digite um nome para um novo grupo.

3. Clique em **Avançar**. A página **Selecionar o servidor e o tipo de produto** é apresentada.

4. Selecione as opções de cenário necessárias, da seguinte forma:

   - Na lista **Selecionar o tipo de servidor**, selecione o tipo de servidor utilizado no cenário.
   - Na opção **Selecionar o tipo de produto**, selecione **Replicação** ou Cenário de alta disponibilidade (HA) de acordo com a licença.
   - **Observação**: para usar a opção **Tarefas na réplica**, consulte o *Guia de Administração do CA ARCserve RHA*.

5. Clique em **Avançar**. A página **Hosts mestre e de réplica** é apresentada.

6. Especifique as seguintes informações:

   - **Nome do cenário** – aceite o nome de cenário padrão ou digite um novo nome para o cenário.
   - **Nome/IP do host mestre** e **Nome/IP do host de réplica** - digite o nome ou IP dos hosts mestre e de réplica ou use o botão **Procurar** para localizá-los.

     Observação: ao criar um cenário de alta disponibilidade é recomendável digitar o endereço IP do host (e não o nome do host).

   - **Credenciais do usuário para verificação de hosts** - digite as credenciais do usuário que permitirão acessar os hosts remotos em que os mecanismos serão instalados.

7. Clique em **Avançar**. A página **Verificação do mecanismo** é apresentada.

   Observação: se a caixa de diálogo **Credenciais do usuário para a verificação de hosts** aparecer, digite as credenciais do usuário que permitirão acessar os hosts remotos em que os mecanismos serão instalados.

8. O sistema verifica a conectividade dos hosts Mestre e de Réplica selecionados na página anterior. Após a verificação das conexões, o sistema verifica se existe um Mecanismo instalado em cada host.

   Observação: uma mensagem de erro indica que não foi possível estabelecer uma conexão ao host especificado. Se algum erro for informado, somente será possível continuar após solucionar o erro.

   Verifique se existe um mecanismo instalado nos hosts selecionados, usando a coluna **Status do servidor**:

   - Se todos os hosts tiverem uma versão como **Instalado**, passe à próxima página.
   - Se algum host estiver marcado como **Não instalado** na coluna Versão atual, será necessário instalar o mecanismo nesses hosts.

     Observação: se um mecanismo não estiver instalado em um ou nos dois hosts e você clicar no botão **Avançar**, a mensagem abaixo aparecerá.

     Clique em **Não** para voltar à página **Verificação do mecanismo** e instalar o mecanismo.

9. Na página **Verificação do mecanismo**, clique no botão **Instalar** para instalar remotamente o mecanismo no host selecionado.

   Observação: você pode instalar o mecanismo nos dois hosts ao mesmo tempo. Para fazer isso, marque as caixas de seleção dos dois hosts e clique no botão **Instalar**.

10. Aguarde até que a instalação seja concluída para ver o número da versão do mecanismo na coluna **Versão atual**.

11. Clique em **Avançar**. A página **Diretórios raiz do mestre** é apresentada.

    Conclua a criação do cenário, seguindo as instruções do assistente. (Para obter mais informações sobre a criação de um novo cenário, consulte o Guia de Administração do *CA ARCserve RHA*.)

Instalar o mecanismo usando o programa de instalação remota

É possível usar o assistente de instalação remota para implantar o mecanismo em vários servidores ou em nós de agrupamentos, executando uma única etapa.

Se um firewall estiver em execução na máquina onde você planeja instalar o mecanismo, deve-se ativar o mecanismo como uma exceção do WMI (Windows Management Instrumentation), na lista de exceções do firewall do Windows. Se o Windows 2003 ou Windows XP estiver em execução, visite o site do Microsoft MSDN e consulte o documento Connecting Through Windows Firewall.

Para instalar o mecanismo com o programa de instalação remota

1. No gerenciador do CA ARCserve RHA, no menu **Ferramentas**, selecione **Executar o programa de instalação remota**.

   A tela do instalador remoto é exibida e o **assistente de instalação remota** aparece, exibindo a página **Seleção do host**.

   Observações:

   - Se no momento você possuir cenários no Gerenciador, os hosts participantes desses cenários aparecerão no painel **Hosts selecionados**. Isso permite atualizar com facilidade a versão do Mecanismo instalada neles.
   - Caso deseje acessar outros recursos do gerenciador enquanto estiver usando o programa de instalação remota, é necessário minimizar o assistente de instalação remota e retorná-lo posteriormente. O assistente está vinculado à exibição do monitor do programa de instalação remota. Se você alternar modos de exibição, o assistente é minimizado automaticamente.

2. Na página **Seleção do host**, selecione os hosts em que deseja instalar o mecanismo. É possível selecionar hosts automática e manualmente:

   - Para detectar automaticamente os hosts existentes no domínio, clique no botão **Iniciar a detecção de hosts**. Os hosts detectados aparecem no painel **Hosts detectados**, à esquerda. Clique duas vezes em um host para selecioná-lo. Ele aparece no painel **Hosts selecionados** à direita.
   - Para selecionar manualmente um host, digite o nome ou o endereço IP do host na caixa **Nome do host/Endereço IP** e clique em **Adicionar**. O host escolhido aparece no painel **Hosts selecionados**.

   Observação: ao usar agrupamentos, você precisa instalar o mecanismo nos dois nós físicos e selecionar um nó físico em vez de um nome de agrupamento.

3. Repita a seleção quantas vezes forem necessárias. O mecanismo será instalado apenas nos servidores apresentados no painel **Hosts selecionados**.

   Observação: para remover hosts do painel **Hosts Selecionados**, selecione os hosts e clique no botão **Remover**.

4. Ao concluir a seleção do host, clique em **Avançar**. A página **Credenciais do usuário** é apresentada.

5. Defina a conta do usuário usada para acessar cada servidor de destino. Você precisa de credenciais de Administrador local para todos os hosts selecionados.

   Observações:

   - É preciso inserir exatamente as mesmas **Credenciais de usuário** utilizadas para efetuar logon no host remoto.
   - Se não for necessário fornecer um valor de domínio para o host selecionado, deixe o campo **Domínio** em branco e digite "**.**" antes do Nome de usuário.

6. Clique em **Avançar**. A página **Verificação anterior à instalação** é apresentada.

   O programa de instalação remota verifica automaticamente a existência de conectividade e a configuração dos servidores selecionados na página anterior. Após a conclusão do processo de verificação, os resultados são exibidos.

   Observação: se o status do servidor foi informado como Erro e você verificou que o servidor existe e está conectado de maneira adequada, selecione-o e clique no botão **Verificar novamente**. O programa de instalação remota repetirá o processo de verificação.

7. Após o status de todos os servidores informar **Não instalado**, clique em **Avançar**.

   Observação: se uma versão anterior do mecanismo foi informada como **Instalado**, desinstale-a clicando no botão **Desinstalar**. Após a conclusão do processo de desinstalação, clique em **Avançar**.

   A página **Configurações de instalação** é apresentada.

   Na seção **Informações de logon de serviço**, selecione **Esta conta** e digite o **Domínio\Nome de usuário** e **Senha** para definir a conta de logon no serviço do mecanismo do CA ARCserve RHA.

Observação: marque a caixa de seleção **Usar as contas de logon no serviço das instalações existentes**, se desejar atualizar um mecanismo existente e permitir que o CA ARCserve RHA use detalhes da conta de logon em que o mecanismo está instalado.

8. Clique em **Avançar**. A página **Pronto para instalação** é apresentada.
9. Verifique se todos os servidores desejados estão listados. A seguir, clique no botão **Instalar** para iniciar a instalação do Mecanismo nesses servidores. Uma mensagem de confirmação é exibida.
10. Clique em **Sim** para instalar o mecanismo. O painel de status do **Instalador remoto** é apresentado. Aguarde o **Status do servidor** ser informado como **Instalado**.
11. Feche o painel de status do **programa de instalação remota**. No modo de exibição do programa de instalação remota, o status de instalação é informado como **Instalação concluída** .

    Agora, o Mecanismo está instalado em todos os servidores ou nós de agrupamentos selecionados.

Instalar o mecanismo usando a CLI

Você pode instalar o mecanismo do CA ARCserve RHA nos servidores mestre e de réplica usando a CLI (Interface de linha de comando).

Para instalar o mecanismo do CA ARCserve RHA usando a CLI

- Abra a CLI e digite o seguinte:

```
CAARCserveRHAEngine.exe /S "/v/qn XOLOGIN="[Domain/UserName]"
XOPASSWORD="[Password]" XOPORT="[Port]" XOLANG="[Language]"
```

Parâmetros

CAARCserveRHAEngine.exe

O arquivo de configuração do mecanismo do CA ARCserve RHA

S, V, QN

Parâmetros de instalação silenciosa

Domain/UserName, Password

Insira as informações necessárias de acordo com a plataforma utilizada e a solução implementada, conforme descrito no capítulo Requisitos de aplicativos e bancos de dados suportados (na página 21). Se você não inserir os detalhes da Conta de logon, o padrão será o Sistema local.

Porta

Digite o número da porta. O padrão é 25000.

Idioma

Selecione o idioma, usando um dos seguintes códigos de idioma:

- "1033" inglês
- "1036" francês
- "1041" japonês
- "2052" chinês (simplificado)
- "1028" chinês (tradicional)
- "1031" alemão
- "1034" espanhol
- "1040" italiano
- "1046" português (Brasil)

Exemplo: instalar o mecanismo usando a CLI

```
CAARCserveRHAEngine.exe /S "/v/qn XOLOGIN="domaun/administrator"
XOPASSWORD="abcd" XOPORT="25000" XOLANG="1033"
```

Instalar e abrir o centro de gerenciamento e o gerenciador

O centro de gerenciamento e o gerenciador não exigem componentes nem aplicativos previamente instalados. É um procedimento de instalação com um único clique que pode ser executado em qualquer estação de trabalho com uma conexão de rede e um navegador da web.

Para instalar o gerenciador:

1. Abra o Internet Explorer. Na caixa **Endereço**, digite o nome do host/endereço IP e o número da porta do serviço de controle, usando este formato: http://host_name:port_no/start_page.aspx

   Observação: se você selecionou a opção **Configuração SSL** durante a instalação do serviço de controle**,** ao abrir a página Visão geral, será necessário usar o nome do host do computador do serviço de controle (em vez do endereço IP). Digite o digite o nome do host e o número da porta do serviço de controle da seguinte maneira: https://host_name:port_no/start_page.aspx

   A caixa de diálogo **Logon** é exibida.

2. Digite seu nome de usuário, senha e domínio e clique em **Logon**.

3. A **Página Visão gera**l é apresentada.

4. Na barra de ferramentas **Início rápido**, clique na opção **Gerenciamento de cenários**.

   Uma barra de andamento é apresentada, indicando que o componente Gerenciador já está instalado no computador local.

5. Concluída a instalação, o gerenciador é apresentado.

   Importante: vários administradores podem acessar o gerenciador do CA ARCserve RHA, ao mesmo tempo, e realizar alterações a qualquer momento que precisarem, dependendo dos seus privilégios. A última atualização será efetivada como o último estado do cenário. Portanto, quando vários administradores trabalham com o gerenciador ao mesmo tempo, é importante estar ciente de que um administrador pode, por engano, substituir as alterações feitas recentemente por outro administrador. Recomenda-se tomar medidas internas para evitar esse tipo de incidente.

Instalar o CA ARCserve RHA para PowerShell

Esta seção descreve como instalar o CA ARCserve RHA para PowerShell.

Para usar o CA ARCserve RHA para PowerShell, é necessário instalar primeiro o Windows PowerShell. Em seguida, instale o CA ARCserve RHA para PowerShell para adicionar snap-ins do CA ARCserve RHA ao conjunto de comandos do PowerShell.

Importante: O CA ARCserve RHA para PowerShell e seu serviço de controle, ao qual está conectado, devem ter a mesma versão.

Para instalar o CA ARCserve RHA para PowerShell:

1. Clique duas vezes no arquivo de instalação **Setup.exe**. O assistente de **instalação do CA ARCserve RHA** é exibido.
2. Clique na opção **Instalar**. A página **Instalar componentes** é exibida.
3. Clique na opção **Instalar o CA ARCserve RHA para PowerShell**. A caixa de diálogo **Escolher idioma de instalação** é exibida.
4. Selecione, na lista suspensa, o idioma do assistente de instalação que preferir e clique em **OK**.

   Uma barra de andamento é apresentada. Após a conclusão do processo inicial, a página **Bem-vindo** é apresentada.
5. Clique em **Avançar**. A página **Contrato de licença** é apresentada.
6. Marque a caixa de seleção **Eu aceito** e clique em **Avançar**. A página **Pasta de destino** é apresentada.
7. Verifique se os detalhes estão corretos nos campos ou altere-os de forma adequada. A seguir, clique em **Avançar**. A página **Pronto para instalar o programa** é exibida.
8. Clique em **Instalar**. Uma barra de andamento é apresentada.
9. Após concluir a instalação, clique em Concluir para terminar a instalação.

Desinstalar o CA ARCserve RHA

A desinstalação de componentes do CA ARCserve RHA é feita de maneira simples e padrão por meio da opção **Adicionar/Remover programas**, na lista do **Painel de controle** do sistema operacional. É preciso desinstalar cada componente do CA ARCserve RHA separadamente.

- A desinstalação não remove o diretório padrão que armazena os arquivos de cenário .xmc gerados pelo usuário e configurados pelo gerenciador do CA ARCserve RHA. O diretório é: *INSTALLDIR*\ *ws_scenarios*.
- Existem dois outros métodos para desinstalar o mecanismo do CA ARCserve RHA. Esses métodos são mais adequados à desinstalação de versões anteriores do Mecanismo:
  - Usando o programa de instalação remota (na página 84)
  - Usando o arquivo Setup.exe (na página 80)

Desinstalar o CA ARCserve RHA para Microsoft Failover Cluster

A desinstalação do CA ARCserve RHA não excluir o recurso de disco CA ARCserve RHA e o tipo de recurso que armazena a configuração.

Para fazer uma desinstalação completa

1. Excluir o recurso de disco do CA ARCserve RHA do armazenamento
2. Use o comando cluster para excluir o tipo de recurso durante a execução do agrupamento.

   ```
   cluster.exe restype "ARCserve Disk" /delete
   ```

Também é possível excluir o tipo de recurso do Microsoft Failover Cluster Manager.

Resolvendo o erro CAVSSSoftProv

Sintoma:

Estou recebendo o seguinte erro ao instalar ou desinstalar o mecanismo do RHA:

```
Erro 27508. Erro ao instalar o aplicativo COM+ CAVSSSoftProv
```

Solução:

Faça o seguinte:

1. Reinicie o sistema operacional.
2. Interrompa o serviço do mecanismo do CA ARCserve RHA.
3. Execute o install_engine.bat a partir do caminho raiz do mecanismo.
4. Execute o uninstall_engine.bat a partir do caminho raiz do mecanismo.
5. Remova o mecanismo usando a opção Adicionar/remover programas.
6. Remova o aplicativo COM+ CAVSSSoftProv.
7. Reinstale o mecanismo do CA ARCserve RHA.

Solução de problemas de verificação do mecanismo do RHA

Sintoma:

No servidor de grupo de trabalho do Windows 2008, o usuário recebe o erro Falha na verificação quando o usuário que efetua logon no servidor é uma conta local no grupo Administrador. O erro é inibido ao verificar o mecanismo do RHA.

Solução:

Para resolver esse problema, desative o UAC ou defina a entrada do Registro, LocalAccountTokenFilterPolicy, como 1.

Para obter mais informações, consulte o artigo 951016 em microsoft.com.

Apêndice B: Instalar o IIS 6.0 Management Compatibility para IIS 7.0/7.5

Esta seção descreve as etapas necessárias para instalar o Management Compatibility do IIS 6.0 para o IIS 7.0./7.5. Esse procedimento é necessário se desejar criar um cenário de alta disponibilidade para o IIS 7.0/7.5.

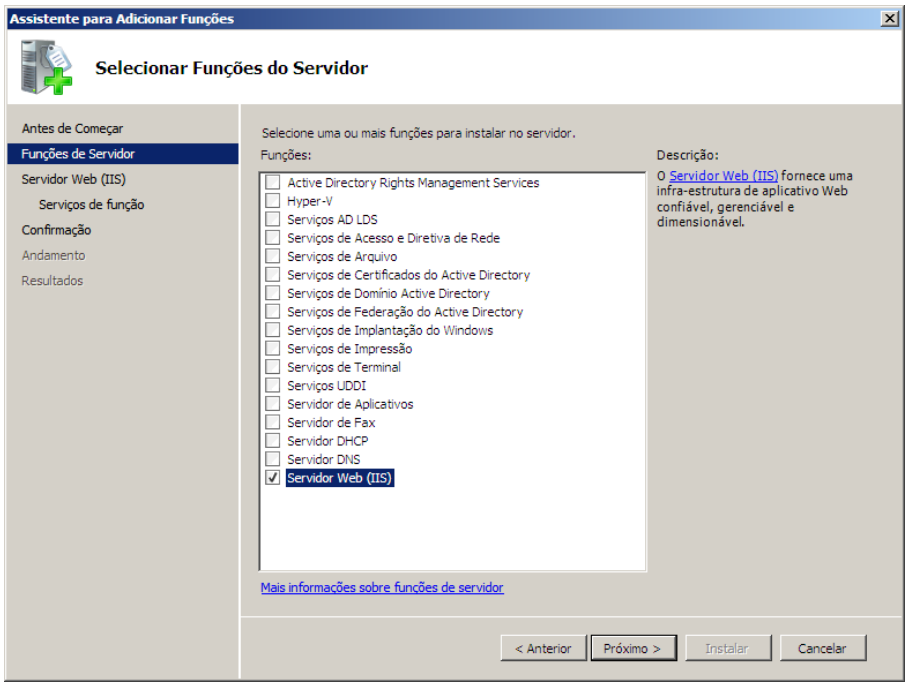
Observação: se pretender criar um cenário de alta disponibilidade para o IIS 7.0/7.5, é necessário repetir este processo nos hosts do mestre e de réplica.

Para instalar o IIS 6.0 Management Compatibility

1. No host mestre ou de réplica, abra o gerenciador do servidor e selecione a opção Roles. Em seguida, clique no botão Add Roles.

   A primeira página do assistente para adicionar funções é exibida.

2. Clique em Avançar. A janela Select Server Roles é exibida.



3. Selecione a caixa de seleção Web Server (IIS) e clique em Next.

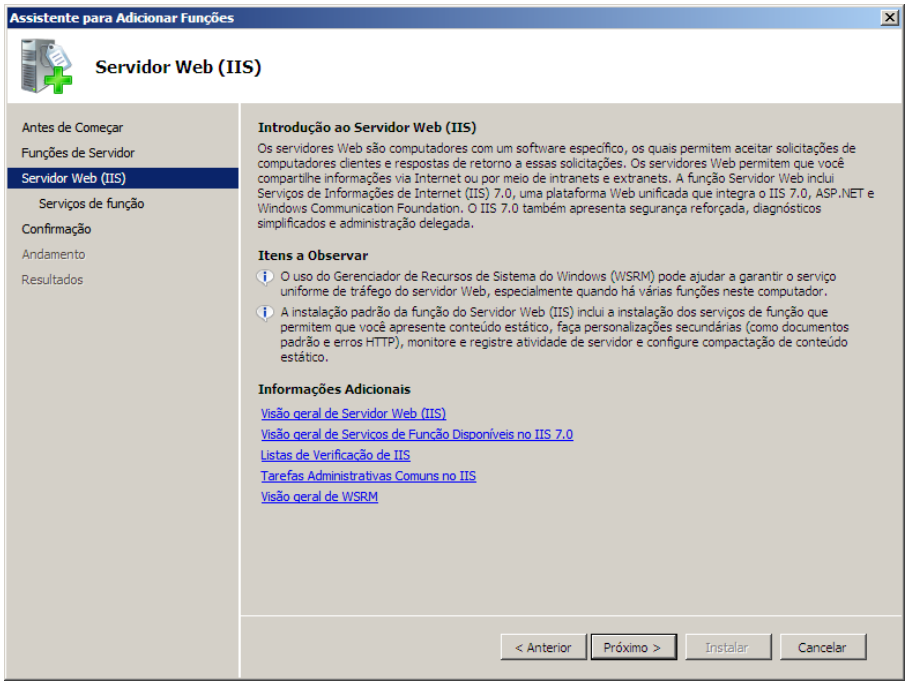
   Uma mensagem pop-up é exibida, perguntando se você deseja adicionar os recursos necessários ao servidor web (IIS).

4. Clique em Add Required Features.

A janela Select Server Roles é exibida.

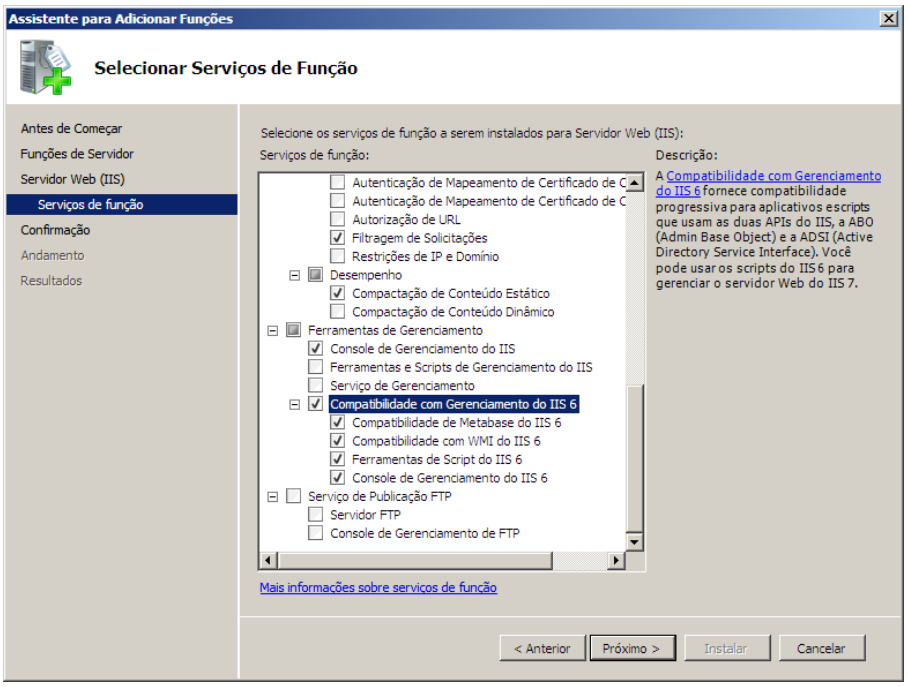
5. Clique em Avançar.

   A janela Web Server (IIS) é exibida.



6. Clique em Avançar.

   A janela Select Role Service é exibida.



7. Na lista de serviços da função, marque a caixa de seleção IIS 6 Management Capability.
8. Clique em Next e siga as instruções do assistente até concluir a instalação.

Apêndice C: Instalação de certificado SSL auto-assinado

Esta seção descreve as etapas necessárias à instalação do Certificado SSL auto-assinado. Este procedimento é necessário ao usar Certificado auto-assinado para manter a segurança da comunicação e ao tentar conectar ao serviço de controle em um computador remoto para abrir a página Visão geral.

Instalação: Certificado auto-assinado

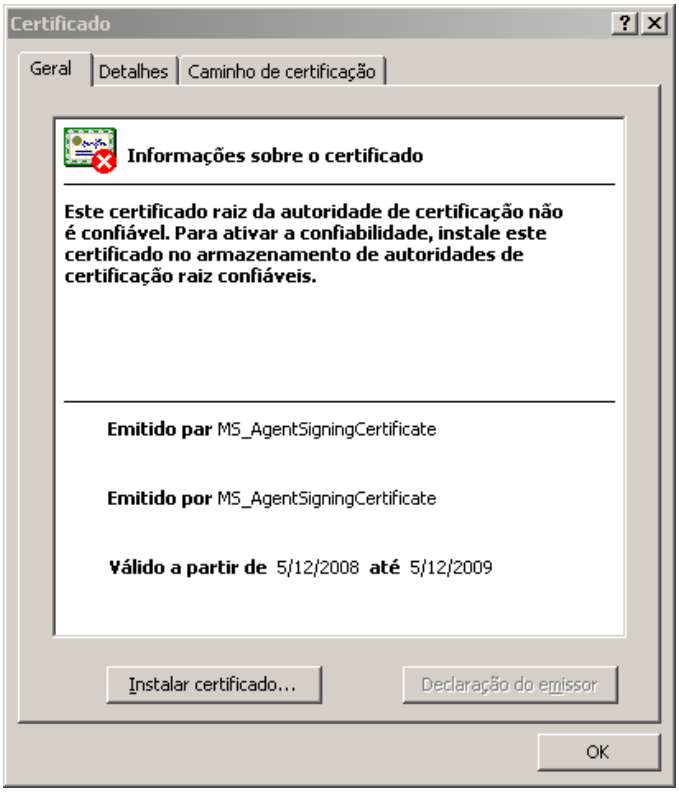
1. No computador remoto, abra o Internet Explorer. Na caixa **Endereço**, digite o nome de host e o número da porta do serviço de controle, usando o seguinte: https://host_name:port_no/start_page.aspx

   Observação: você não pode usar aqui o endereço IP do serviço de controle.

   Um alerta de segurança aparece, perguntando se você deseja exibir o certificado.

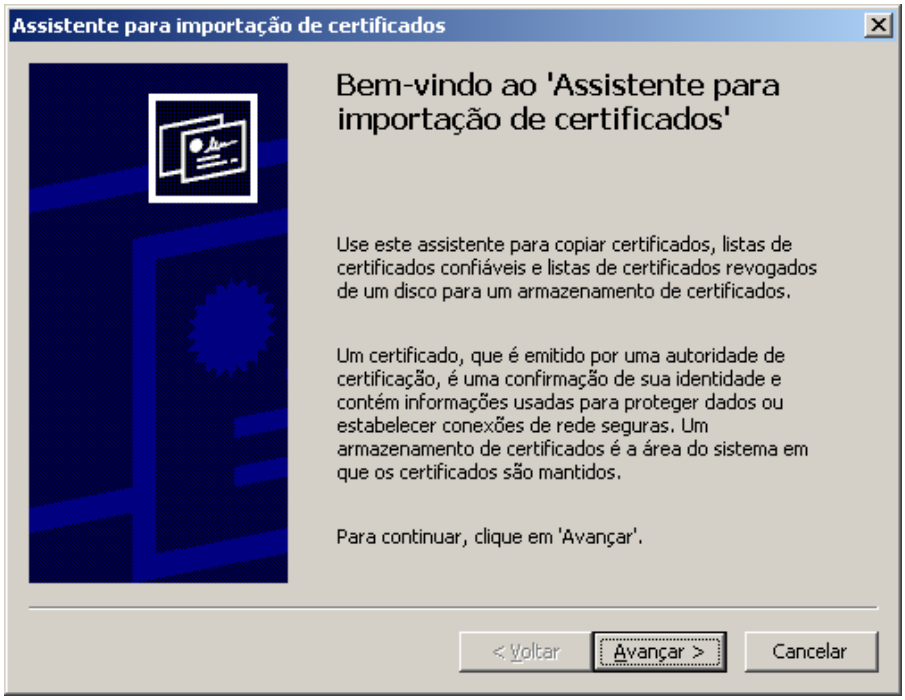
2. Clique no botão **Exibir certificado**.

   A caixa de diálogo **Certificado** é apresentada:

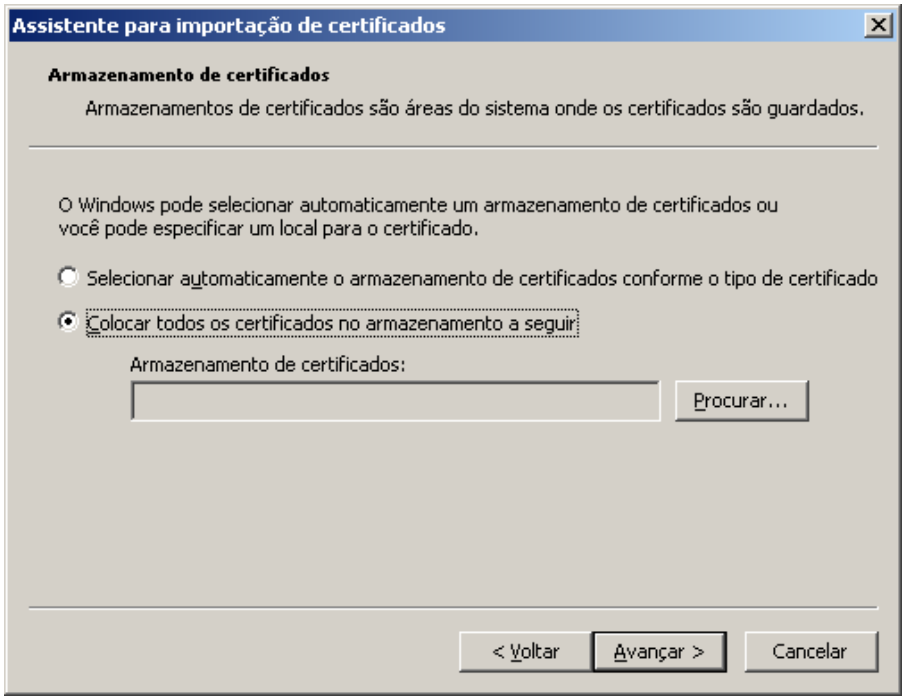


3. Para instalar localmente o certificado, clique no botão **Instalar certificado**.

   O **Assistente para importação de certificados** é apresentado:



4. Clique em **Avançar**. A página **Armazenamento de certificados** é apresentada:

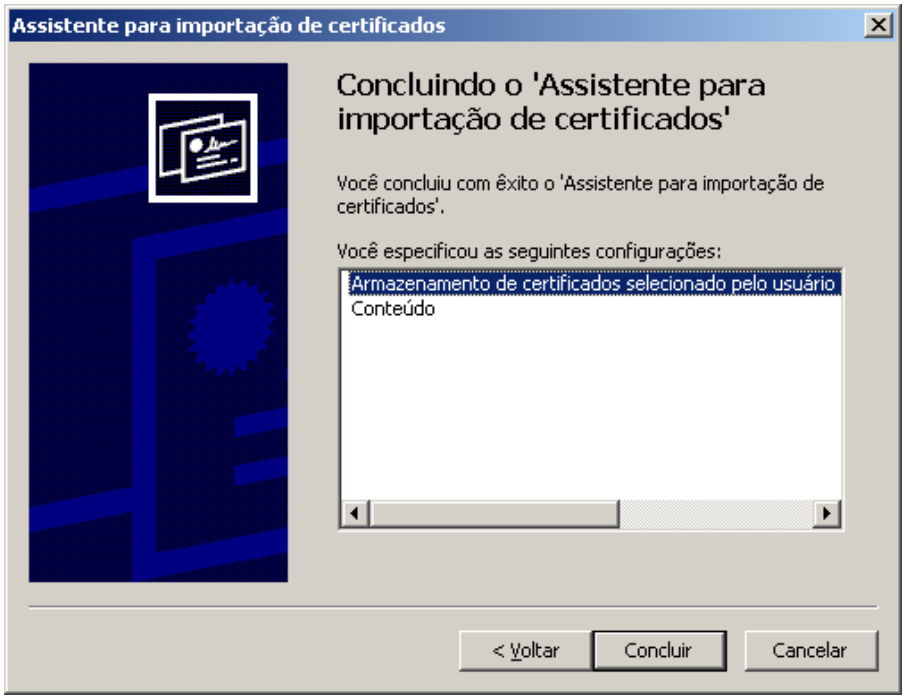


5. Selecione o botão de opção **Colocar todos os certificados no seguinte armazenamento** e clique no botão **Procurar**.

   A caixa de diálogo **Selecionar armazenamento do certificado** é apresentada:

6. Selecione o armazenamento **Autoridades de certificação raiz confiáveis** e clique em **OK**.

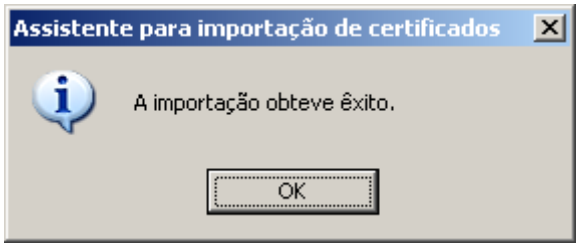
   A página **Conclusão do Assistente para importação de certificados** é apresentada:



7. Clique em **Concluir** para terminar a importação do certificado.

   Uma mensagem de confirmação é apresentada, solicitando que você confirme a instalação do certificado.

8. Clique em **Sim**. Uma mensagem aparece, informando o sucesso da importação:



9. Clique em **OK** para fechar a mensagem. Na caixa de diálogo **Certificado**, clique em **OK** para fechá-la.

   Agora você pode se conectar ao computador do Serviço de controle e abrir a página Visão geral.

Apêndice D: Renovar um certificado SSL expirado

Esta seção descreve as etapas necessárias para renovar um certificado SSL expirado, autorizado ou auto-assinado. Esse procedimento é necessário caso já esteja usando o certificado SSL para proteger a comunicação, o certificado atual esteja expirado e você deseja instalar um novo certificado.

Observação: não é necessário interromper o serviço de controle durante o processo de renovação.

Para renovar um certificado SSL expirado

1. Obtenha um novo certificado e instale-o na máquina na qual o serviço de controle esteja em execução.
2. Para remover a associação do certificado antigo, execute o seguinte comando:

   ```
   httpcfg.exe delete ssl -i 0,0.0,0:{CS SSL Port Number}
   ```

   Observação: o parâmetro **CS SSL Port Number** corresponde ao número da porta fornecido durante a instalação do serviço de controle. Você pode encontrar este valor no arquivo **ws_man.exe.config**, no valor **ws_port**.

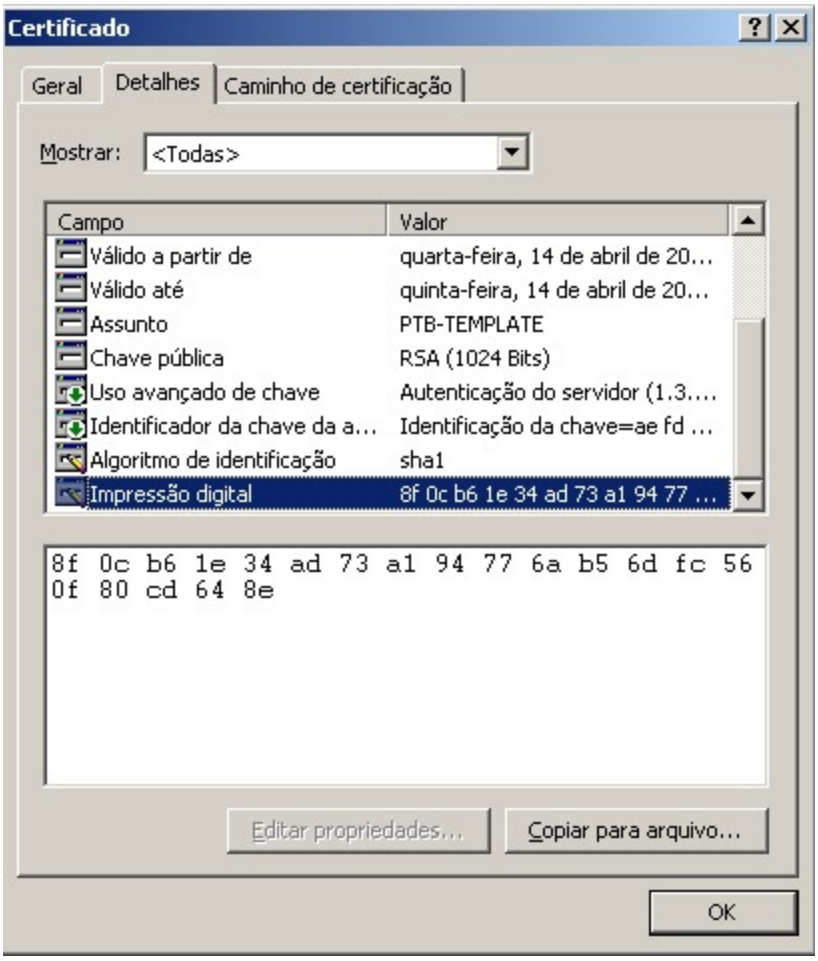
   O comando não pode resultar em erros. E o final da mensagem deverá ser:

   …completed with 0.
3. Para associar o novo certificado à porta SSL do serviço de controle, execute o seguinte comando:

   ```
   httpcfg.exe set ssl -i 0,0.0,0:{CS SSL Port Number} -h {New Certificate SslHash}
   ```

Observações:

- O parâmetro **httpcfg.exe** é um utilitário padrão para Windows Servers, e você pode encontrá-lo no diretório de instalação do serviço de controle.
- É possível encontrar o parâmetro **New Certificate SSlHash** na caixa de diálogo **Certificate**, da guia **Details**, no valor **Thumbprint**.



Lembre-se de inserir o valor Thumbprint sem espaços entre os caracteres, conforme abaixo: 8f40f9904372ccbd3706d72ed25d.

O comando não pode resultar em erros. O final da mensagem deverá ser:

…completed with 0.

Isso feito, o certificado SSL estará renovado.

Apêndice E: Instalando o cliente Oracle para suportar Oracle de 32 bits no sistema operacional de 64 bits

Se estiver usando o Oracle 32 bits no SO 64 bits, você precisa instalar o cliente Oracle 11.x ou superior no computador Oracle para executar o cenário Oracle com êxito.

Para instalar o cliente Oracle 11.x

1. Faça download do cliente Oracle 11.x a partir do seguinte endereço:

   http://www.oracle.com/technology/software/tech/oci/instantclient/htdocs/winx64soft.html

2. Instale o **Pacote básico do Instant Client** no diretório atual de instalação do mecanismo ou em um dos caminhos padrão do sistema operacional.

Apêndice F: Reconhecimentos

Partes deste produto incluem software desenvolvido por fornecedores de softwares de terceiros. A seção a seguir fornece informações referentes a esse software de terceiros.

Esta seção contém os seguintes tópicos:

Reconhecimento do ISC bind 9.3.2

Bind 9.3.2 copyright message Copyright (C) 2004, 2005 Internet Systems Consortium, Inc. ("ISC") Copyright (C) 1996-2003 Internet Software Consortium.

Este produto inclui software desenvolvido pela ISC. O software da ISC é distribuído de acordo com o seguinte contrato de licença:

Por meio deste, concedemos permissão para usar, copiar, modificar e distribuir este software para qualquer propósito, com ou sem cobrança de taxa, desde que o aviso de direitos autorais e este aviso de permissão constem em todas as cópias.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Reconhecimento do CAPICOM 2.1.0.1

Este produto contém uma cópia do Microsoft CAPICOM 2.1.0.1. Sendo assim, todos os títulos, direitos e interesses pertencem à Microsoft Corporation.

CONTRATO DE LICENÇA DE USUÁRIO FINAL DO KIT DE DESENVOLVIMENTO DE SOFTWARE DA PLATAFORMA MICROSOFT

IMPORTANTE - LEIA COM CUIDADO: Este contrato de licença do usuário final da Microsoft ("EULA") é um contrato legal entre você (indivíduo ou entidade individual) e a Microsoft Corporation relativo ao software da Microsoft identificado acima, que inclui software e pode incluir mídia associada, materiais impressos e documentação "online" ou eletrônica ("SOFTWARE"). Uma emenda ou adendo a este EULA pode acompanhar o SOFTWARE. AO INSTALAR, COPIAR OU UTILIZAR O SOFTWARE, VOCÊ CONCORDA EM CUMPRIR OS TERMOS DESTE EULA. CASO NÃO ESTEJA DE ACORDO, NÃO INSTALE OU UTILIZE O SOFTWARE. DEVOLVA-O AO LOCAL DA COMPRA PARA OBTER UM REEMBOLSO TOTAL.

1. CONCESSÃO DE LICENÇA. A Microsoft concede a você os seguintes direitos, desde que você cumpra a todos os termos e condições deste EULA:

* SOFTWARE. Você poderá instalar e usar um número ilimitado de cópias do SOFTWARE em computadores, incluindo estações de trabalho, terminais ou outros dispositivos eletrônicos digitais ("Computadores") para elaborar, desenvolver e testar seu(s) aplicativo(s) de software ("Aplicativo") para uso com qualquer versão ou edição de produtos dos sistemas operacionais Microsoft Windows 95, Windows 98, Windows NT 4.0, Windows 2000 e/ou qualquer versão ou edição de qualquer produto de sistema operacional Microsoft superior ao acima exposto e/ou qualquer conjunto de produtos da Microsoft que contenha algum dos expostos acima (cada um "Produto do sistema operacional Microsoft").

* Código Amostra. Você pode modificar o código-fonte de amostra, localizado nos diretórios de “amostras” do SOFTWARE ("Código Amostra") para elaborar, desenvolver e testar o Aplicativo somente para uso com um produto do sistema operacional Microsoft. Você também pode reproduzir e distribuir o Código Amostra, junto com quaisquer modificações nele feitas, contanto que atenda aos Termos de distribuição descritos abaixo. Para os propósitos desta seção, “modificações” significa aprimoramentos das funções do Código Amostra.

* Código redistribuível. Partes do SOFTWARE são conhecidas como "Código redistribuível". O arquivo de texto \LICENSE\REDIST.TXT lista o código redistribuível e descreve os direitos de distribuição associados a ele, objeto também dos Termos de distribuição especificados abaixo.

* Termos de distribuição. Você pode reproduzir ou distribuir um número ilimitado de cópias do Código Amostra e/ou do Código redistribuível (coletivamente chamados de “Componentes redistribuíveis”), contanto que (a) distribua os componentes redistribuíveis somente em conjunto com o Aplicativo ou como parte dele, para uso com um produto do sistema operacional Microsoft; (b) o Aplicativo acrescente funcionalidade significativa e fundamental aos componentes redistribuíveis; (c) distribua o Aplicativo com componentes redistribuíveis que estejam de acordo com um Contrato de licença de usuário final (que pode ser "break-the-seal", "click-wrap" ou assinado), contendo termos que ofereçam pelo menos o mesmo grau de proteção aqui contido; (d) não autorize redistribuição adicional pelos seus usuários finais; (e) não use o nome, logotipo ou marca registrada da Microsoft para comercializar o Aplicativo; (f) inclua um aviso de direitos autorais válido no Aplicativo e (g) concorde em indenizar, resguardar e defender a Microsoft contra toda e qualquer demanda ou ação, incluindo honorários advocatícios, que possam decorrer do uso ou distribuição do aplicativo. Entre em contato com a Microsoft para obter informações sobre termos de licença aplicáveis para todos os outros usos e/ou distribuição dos componentes redistribuíveis.

* Direitos reservados. Todos os direitos que não estejam expressamente concedidos neste EULA são reservados à Microsoft.

* Código de pré-lançamento. O SOFTWARE pode conter código de pré-lançamento que não atinge o nível de desempenho e compatibilidade do produto final de disponibilidade geral. Essas partes do SOFTWARE podem não operar corretamente e podem ser substancialmente modificadas antes do primeiro lançamento comercial. A Microsoft não está obrigada a tornar comercialmente disponível o SOFTWARE ou qualquer versão posterior. A Microsoft garante a você o direito de distribuir a versão de teste de seu Aplicativo criado com o CÓDIGO DE PRÉ-LANÇAMENTO, contanto que você atenda aos requisitos de distribuição descritos na Seção 1 e as seguintes disposições adicionais: (a) você deve marcar a versão de teste de seu aplicativo como "BETA" e (b) você é exclusivamente responsável por atualizar seus clientes com versões de seu Aplicativo que operem satisfatoriamente com a versão comercial final do CÓDIGO DE PRÉ-LANÇAMENTO.

2. CONFIDENCIALIDADE DO CÓDIGO DE PRÉ-LANÇAMENTO. O CÓDIGO DE PRÉ-LANÇAMENTO, incluindo seus recursos, é propriedade e informação confidencial da Microsoft e seus fornecedores. você concorda em não divulgar ou fornecer o CÓDIGO DE PRÉ-LANÇAMENTO, documentação ou qualquer informação relacionada ao CÓDIGO DE PRÉ-LANÇAMENTO (incluindo recursos ou resultado de uso ou de teste) a terceiros, exceto conforme descrito aqui, sem a permissão escrita expressa da Microsoft. Porém, você pode divulgar informações confidenciais de acordo com ordem judicial ou governamental, contanto que forneça à Microsoft um aviso prévio razoável para tal divulgação e esteja de acordo com qualquer solicitação protetora aplicável ou equivalente. Você não deve ser responsabilizado perante a Microsoft pelas informações que puder provar que (1) já eram de seu conhecimento; (2) se tornaram publicamente conhecidas sem qualquer ato ilegal realizado por você; (3) forem legalmente recebidas de terceiros sem restrição semelhante e sem quebra deste contrato; ou (4) sejam independentemente desenvolvidas por você. Essa disposição prevalecerá sobre o término ou expiração deste contrato.

3. TRANSFERÊNCIA Interna. Você pode transferir o SOFTWARE para um outro computador. Transferência para terceiros. O usuário inicial do SOFTWARE deve fazer uma única transferência deste para outro usuário final. A transferência deve incluir todas as partes do componente, mídia, materiais impressos, este EULA, se aplicável, e o Certificado de Autenticidade. A transferência não deve ser indireta, tal como uma consignação. Antes dela, o usuário final que receber o SOFTWARE a ser transferido deve concordar com todos os termos do EULA. Sem aluguel. Você não deve alugar, arrendar ou emprestar o SOFTWARE.

4. LIMITAÇÕES DE ENGENHARIA REVERSA, DESCOMPILAÇÃO E DESMONTAGEM. Não será permitido fazer engenharia reversa, descompilar ou desmontar o SOFTWARE, exceto e somente na medida em que tal atividade seja expressamente permitida pela legislação aplicável, não obstante esta limitação.

5. RESCISÃO. Sem prejudicar quaisquer outros direitos, a Microsoft pode cancelar este EULA se você não cumprir seus termos e condições, caso em que você deve destruir todas as cópias do SOFTWARE e todos os seus componentes.

6. CONSENTIMENTO PARA O USO DE DADOS. Você concorda que a Microsoft e suas afiliadas podem coletar e usar informações técnicas oferecidas por você como parte dos serviços de suporte relacionados ao SOFTWARE. A Microsoft concorda em não usar essas informações de forma a identificá-lo pessoalmente.

7. SOFTWARE NÃO DISPONÍVEL PARA VENDA. O SOFTWARE identificado como “Não disponível para revenda” ou “NFR", não deve ser revendido, transferido ou usado para qualquer finalidade que não seja para demonstração, teste ou avaliação.

8. SOFTWARE DE EDIÇÃO ACADÊMICA. Para usar um Produto identificado como “Edição Acadêmica ou "AE," você deve ser um “Usuário Educacional Qualificado”. Para questões referentes à qualificação, entre em contato com o Microsoft Sales Information Center/One Microsoft Way/Redmond, WA 98052-6399 ou uma subsidiária da Microsoft que atenda o seu país.

9. RESTRIÇÕES DE EXPORTAÇÃO. Você reconhece que este SOFTWARE é de origem americana. Você concorda em cumprir com todas as leis nacionais e internacionais que se aplicarem ao SOFTWARE, incluindo as regras de administração de exportação americanas, bem como as restrições do usuário final, de uso final e de destinação emitidas pelos EUA. Para obter mais informações, consulte .

10. DECLARAÇÃO DE ISENÇÃO DE GARANTIAS. Até a extensão máxima permitida pela lei aplicável, a Microsoft e seus fornecedores fornecem o SOFTWARE e quaisquer serviços de suporte (se houver) relacionados ao SOFTWARE ("Serviços de suporte") COMO ESTÃO E COM TODAS AS FALHAS; e a Microsoft e seus fornecedores renunciam aqui com respeito ao SOFTWARE e aos Serviços de suporte a todas as garantias e condições, expressas, implícitas ou estabelecidas por lei, incluindo, sem limitação, quaisquer garantias (se houver), responsabilidades ou condições de ou relacionado a: comercialização, adequação para uma finalidade específica, falta de vírus, precisão ou totalidade de respostas, resultados, esforço técnico ou falta de negligência. TAMBÉM NÃO HÁ GARANTIA, OBRIGAÇÃO OU CONDIÇÃO DE TITULARIDADE, USO PACÍFICO, POSSE PACÍFICA, CORRESPONDÊNCIA À DESCRIÇÃO OU NÃO-VIOLAÇÃO. VOCÊ ASSUME TODOS OS RISCOS RESULTANTES DO USO OU DO DESEMPENHO DO SOFTWARE E DE QUALQUER SERVIÇO DE SUPORTE.

11. EXCLUSÃO DE DANOS INCIDENTAIS, INDIRETOS E OUTROS ESPECÍFICOS. ATÉ A EXTENSÃO MÁXIMA PERMITIDA PELA LEI APLICÁVEL, EM HIPÓTESE ALGUMA A MICROSOFT OU SEUS FORNECEDORES PODEM SER RESPONSABILIZADOS POR QUALQUER DANO ESPECIAL, ACIDENTAL, INDIRETO, PUNITIVO OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÃO, DANOS POR: LUCRO CESSANTE, PERDA DE INFORMAÇÕES CONFIDENCIAIS OU OUTRAS INFORMAÇÕES, INTERRUPÇÃO DOS NEGÓCIOS, ACIDENTE PESSOAL, PERDA DE PRIVACIDADE, FALHA EM ATENDER A ALGUMA RESPONSABILIDADE (INCLUINDO DE BOA FÉ OU DE CUIDADOS RAZOÁVEIS), NEGLIGÊNCIA E QUALQUER OUTRA PERDA FINANCEIRA OU DE QUALQUER OUTRO TIPO) RESULTANTES DO, OU DE QUALQUER FORMA RELACIONADOS AO, USO OU IMPOSSIBILIDADE DE USO DO SOFTWARE OU DOS SERVIÇOS DE SUPORTE, OU DO FORNECIMENTO, OU FALHA NO FORNECIMENTO, DOS SERVIÇOS DE SUPORTE OU SOB OU COM RELAÇÃO A QUALQUER DISPOSIÇÃO DESTE EULA, MESMO SE A MICROSOFT OU QUALQUER FORNECEDOR TIVER SIDO AVISADO SOBRE A POSSIBILIDADE DE TAIS DANOS.

12. LIMITAÇÃO DE RESPONSABILIDADE E REMÉDIOS. Não obstante quaisquer danos que você possa sofrer por qualquer razão (incluindo, entre outros, todos os danos relacionados acima e todos os danos diretos ou gerais), a responsabilidade total da Microsoft e de qualquer de seus fornecedores de acordo com qualquer disposição deste EULA e seu recurso exclusivo em relação ao supracitado serão limitados à quantia máxima realmente paga pelo SOFTWARE ou US$ 5,00. As limitações, exclusões e isenções supracitadas aplicam-se à extensão máxima permitida pela legislação aplicável, mesmo no caso de algum remédio não servir ao seu propósito essencial.

13. OBSERVAÇÃO SOBRE O SUPORTE JAVA. O SOFTWARE PODE CONTER SUPORTE PARA PROGRAMAS ESCRITOS EM LINGUAGEM JAVA. A TECNOLOGIA JAVA NÃO É TOLERANTE A ERROS E NÃO FOI ELABORADA, FABRICADA OU DESTINADA PARA O USO OU REVENDA COMO EQUIPAMENTO DE CONTROLE ONLINE EM AMBIENTES PERIGOSOS QUE EXIJAM DESEMPENHOS LIVRES DE FALHAS, TAIS COMO OPERAÇÃO DE INSTALAÇÕES NUCLEARES, SISTEMAS DE NAVEGAÇÃO OU DE COMUNICAÇÃO DE AERONAVES, CONTROLE DE TRÁFEGO AÉREO, MÁQUINAS DE APOIO DIRETO À VIDA OU SISTEMAS DE ARMAZENAMENTO, NOS QUAIS UMA FALHA DA TECNOLOGIA JAVA PODERIA CONDUZIR DIRETAMENTE À MORTE, LESÃO CORPORAL, OU DANOS FÍSICOS OU AMBIENTAIS GRAVES. A Sun Microsystems, Inc. obrigou contratualmente a Microsoft a incluir essa exoneração de responsabilidade.

14. DIREITOS DE LICENÇA DO GOVERNO DOS EUA. Todo SOFTWARE fornecido nos EUA, de acordo com as solicitações emitidas em 1 de dezembro de 1995 ou após esta data, receberá os direitos de licença comercial, bem como as restrições descritas neste documento. Todo SOFTWARE fornecido nos EUA, de acordo com as solicitações emitidas antes de 1 de dezembro de 1995, possui "Direitos restritos" conforme o disposto na FAR, 48 CFR 52.227-14 (JUNHO DE 1987) ou na DFAR, 48 CFR 252.227-7013 (OUTUBRO DE 1988), conforme aplicável.

15. LEGISLAÇÃO APLICÁVEL. Se este SOFTWARE for adquirido nos Estados Unidos, este EULA será regido pelas leis do Estado de Washington. Caso este SOFTWARE seja adquirido no Canadá, a menos que expressamente proibido pela legislação local, este EULA será regido pelas leis em vigor na Província de Ontário, Canadá; e, em relação a qualquer disputa que possa surgir em decorrência deste, fica sujeito à jurisdição dos tribunais federais e das províncias estabelecidos em Toronto, Ontário. Caso este SOFTWARE seja adquirido fora dos Estados Unidos, a legislação local será aplicada.

16. TOTALIDADE DO ACORDO. Este EULA (incluindo qualquer adendo ou emenda feita neste EULA incluído no SOFTWARE) é o acordo completo entre você e a Microsoft em relação ao SOFTWARE e aos serviços de suporte (se houver) e prevalecerá sobre todas as comunicações verbais ou escritas, propostas ou representações com respeito ao SOFTWARE ou a qualquer outro assunto coberto por este EULA. Na medida em que os termos de quaisquer políticas ou programas de serviços de suporte da Microsoft entrarem em conflito com os termos deste EULA, os termos deste documento prevalecerão.

17. O SOFTWARE é protegido pelos direitos autorais e outras leis e tratados de propriedade intelectual. A Microsoft ou seus fornecedores possuem a titularidade, os direitos autorais e outros direitos de propriedade intelectual do SOFTWARE. O SOFTWARE é licenciado, não vendido.

Todos os direitos autorais e outros avisos contidos no CAPICOM devem permanecer integralmente com tal componente.

Reconhecimento do Zlib 1.2.3

/* zlib.h -- interface do 'zlib', biblioteca compactada de finalidade geral, versão 1.1.4, 11 de março de 2002

Copyright (C) 1995-2004 Jean-loup Gailly e Mark Adler

Este software é fornecido 'como está', sem qualquer garantia expressa ou implícita. Em hipótese alguma os autores serão responsabilizados por quaisquer danos resultantes do uso deste software.

A permissão de uso deste software é concedida a todos para qualquer fim, incluindo fins comerciais, e também é concedida para alterá-lo e redistribui-lo livremente, sujeito às seguintes restrições:

1. A origem deste software não deve ser apresentada de forma inadequada; você não pode reivindicar a autoria do software original. Se você usar este software em um produto, um reconhecimento na documentação do produto será bem-vindo, porém não é obrigatório.

2. As versões de código fonte alterado devem ser marcadas como tal, e não devem ser apresentadas de forma inadequada como sendo o software original.

3. Esse aviso não pode ser removido ou alterado de nenhuma fonte distribution.Acknowledgement

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

OpenSSL 1.0.0d Acknowledgement

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/) and distributed in accordance with the following licensing terms:

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

Licença da OpenSSL

```
/*
=====================================================================
===
 * Copyright (c) 1998-2011 The OpenSSL Project.  Todos os direitos reservados.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
```

```
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
```

```
 *

 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY

 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR

 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR

 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,

 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT,

 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED

 * OF THE POSSIBILITY OF SUCH DAMAGE.

 *
================================================================
===

 *

 * This product includes cryptographic software written by Eric Young

 * (eay@cryptsoft.com).  This product includes software written by Tim

 * Hudson (tjh@cryptsoft.com).

 *

 */
```

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

*

* This package is an SSL implementation written

* by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscapes SSL.

*

* This library is free for commercial and non-commercial use as long as

* the following conditions are aheared to. The following conditions

* apply to all code found in this distribution, be it the RC4, RSA,

* lhash, DES, etc., code; not just the SSL code. The SSL documentation

* included with this distribution is covered by the same copyright terms

* except that the holder is Tim Hudson (tjh@cryptsoft.com).

*

* Copyright remains Eric Young's, and as such any Copyright notices in

* the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution

* as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or

* in documentation (online or textual) provided with the package.

*

* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE

* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS

* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF

* SUCH DAMAGE.

*

* The licence and distribution terms for any publically available version or

* derivative of this code cannot be changed. i.e. this code cannot simply be

* copied and put under another distribution licence

* [including the GNU Public Licence.]

*/

Índice remissivo

H

I

M

N

P

R

S

W