

CA ARCserve® Replication and High Availability

Guia de Operações para UNIX e Linux

r16



A presente documentação, que inclui os sistemas de ajuda incorporados e os materiais distribuídos eletronicamente (doravante denominada Documentação), destina-se apenas a fins informativos e está sujeita a alterações ou revogação por parte da CA a qualquer momento.

A Documentação não pode ser copiada, transferida, reproduzida, divulgada, modificada ou duplicada, no todo ou em parte, sem o prévio consentimento por escrito da CA. A presente Documentação contém informações confidenciais e de propriedade da CA, não podendo ser divulgadas ou usadas para quaisquer outros fins que não aqueles permitidos por (i) um outro contrato celebrado entre o cliente e a CA que rege o uso do software da CA ao qual a Documentação está relacionada; ou (ii) um outro contrato de confidencialidade celebrado entre o cliente e a CA.

Não obstante o supracitado, se o Cliente for um usuário licenciado do(s) produto(s) de software constante(s) na Documentação, é permitido que ele imprima ou, de outro modo, disponibilize uma quantidade razoável de cópias da Documentação para uso interno seu e de seus funcionários referente ao software em questão, contanto que todos os avisos de direitos autorais e legendas da CA estejam presentes em cada cópia reproduzida.

O direito à impressão ou, de outro modo, à disponibilidade de cópias da Documentação está limitado ao período em que a licença aplicável ao referido software permanecer em pleno vigor e efeito. Em caso de término da licença, por qualquer motivo, fica o usuário responsável por garantir à CA, por escrito, que todas as cópias, parciais ou integrais, da Documentação sejam devolvidas à CA ou destruídas.

NA MEDIDA EM QUE PERMITIDO PELA LEI APLICÁVEL, A CA FORNECE ESTA DOCUMENTAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM NENHUM TIPO DE GARANTIA, INCLUINDO, ENTRE OUTROS, QUAISQUER GARANTIAS IMPLÍCITAS DE COMERCIALIZIDADE, ADEQUAÇÃO A UM DETERMINADO FIM OU NÃO VIOLAÇÃO. EM NENHUMA OCASIÃO, A CA SERÁ RESPONSÁVEL PERANTE O USUÁRIO OU TERCEIROS POR QUAISQUER PERDAS OU DANOS, DIRETOS OU INDIRETOS, RESULTANTES DO USO DA DOCUMENTAÇÃO, INCLUINDO, ENTRE OUTROS, LUCROS CESSANTES, PERDA DE INVESTIMENTO, INTERRUÇÃO DOS NEGÓCIOS, FUNDO DE COMÉRCIO OU PERDA DE DADOS, MESMO QUE A CA TENHA SIDO EXPRESSAMENTE ADVERTIDA SOBRE A POSSIBILIDADE DE TAIS PERDAS E DANOS.

O uso de qualquer produto de software mencionado na Documentação é regido pelo contrato de licença aplicável, sendo que tal contrato de licença não é modificado de nenhum modo pelos termos deste aviso.

O fabricante desta Documentação é a CA.

Fornecida com "Direitos restritos". O uso, duplicação ou divulgação pelo governo dos Estados Unidos está sujeita às restrições descritas no FAR, seções 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e DFARS, seção 252.227-7014(b)(3), conforme aplicável, ou sucessores.

Copyright © 2012 CA. Todos os direitos reservados. Todas as marcas comerciais, nomes de marcas, marcas de serviço e logotipos aqui mencionados pertencem às suas respectivas empresas.

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA ARCserve® Replication
- CA ARCserve® High Availability (HA)

Em todo este guia, o nome 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>.

Índice

Capítulo 1: Introdução	7
Documentação relacionada	7
Tipos de servidor suportados	7
Capítulo 2: Instalando e desinstalando o CA ARCserve RHA	9
Instalar o mecanismo.....	10
Para instalar o mecanismo em zonas não globais no Solaris.....	11
Gerenciando o mecanismo	11
Instalando o gerenciador.....	12
Prepare o ambiente de alta disponibilidade com o script GSSnsupdate.....	14
Atualizando o CA ARCserve RHA.....	17
Desinstalando o CA ARCserve RHA.....	17
Desinstalar o CA ARCserve RHA	18
Capítulo 3: Métodos de redirecionamento	19
Capítulo 4: Gerenciando cenários	21
Criar um cenário de replicação do UNIX.....	22
Para criar um cenário de alta disponibilidade do UNIX.....	26
Iniciar um cenário	28
Interromper um cenário	30
Considerações sobre o cenário no UNIX/Linux.....	31
Apêndice A: Arquivos instalados	33
Arquivos instalados no Red Hat e Novell SUSE Linux Enterprise.....	33
Arquivos instalados no IBM AIX.....	34
Arquivos instalados no Solaris	35
Apêndice B: Solução de problemas	37
Descarregar drivers do xofs	37

Capítulo 1: Introdução

Este documento é destinado aos administradores experientes do sistema UNIX e Linux que estejam interessados na implementação e implantação, em seus ambientes, da solução CA ARCserve RHA. O documento fornece todos os detalhes necessários para instalar e desinstalar o produto, criar cenários de replicação (recuperação de falhas) e de alta disponibilidade, bem como, gerenciar cenários e recuperar dados perdidos.

Esta seção contém os seguintes tópicos:

[Documentação relacionada](#) (na página 7)

[Tipos de servidor suportados](#) (na página 7)

Documentação relacionada

Use este Guia com o *Guia de Instalação do CA ARCserve RHA*, o *Guia de Administração do CA ARCserve RHA* e o *Guia dos Comandos do CA ARCserve RHA PowerShell*.

Tipos de servidor suportados

Consulte as Notas da Versão para saber quais são os tipos de servidor com suporte.

Capítulo 2: Instalando e desinstalando o CA ARCserve RHA

Este capítulo explica como instalar e desinstalar o mecanismo do CA ARCserve RHA e o gerenciador do CA ARCserve RHA.

Esta seção contém os seguintes tópicos:

[Instalar o mecanismo](#) (na página 10)

[Gerenciando o mecanismo](#) (na página 11)

[Instalando o gerenciador](#) (na página 12)

[Prepare o ambiente de alta disponibilidade com o script GSSnupdate](#) (na página 14)

[Atualizando o CA ARCserve RHA](#) (na página 17)

[Desinstalando o CA ARCserve RHA](#) (na página 17)

Instalar o mecanismo

O pacote de instalação do CA ARCserve RHA consiste em pacotes para todas as plataformas suportadas e um script de instalação comum.

Para instalar o mecanismo

1. Torne-se um "superusuário" (raiz).
2. Altere o diretório de trabalho para ser o diretório que contém os arquivos de instalação
3. Execute o script *install.sh*.
4. Siga as instruções até o final da instalação.

Você deve aceitar o contrato de licença e decidir se deseja criar o grupo do CA ARCserve RHA ou ativar o suporte a Oracle.

Observações:

- Se você optar por ativar o suporte a Oracle, é necessário fornecer o proprietário, o caminho inicial e o caminho base do Oracle. O usuário proprietário do Oracle é solicitado primeiro e, em seguida, o produto recupera o caminho inicial e o caminho base por meio do ambiente do usuário proprietário. Se o caminho inicial e o caminho base não puderem ser encontrados, é necessário adicioná-los manualmente. Se o seu servidor Oracle estiver instalado sem a biblioteca cliente do Oracle de 32 bits, você também deverá fornecer o caminho do Oracle Instant Client.
- Se o pacote do CA ARCserve RHA tiver sido instalado, será necessário instalá-lo novamente.
- Para permitir que usuários fora da raiz gerenciem cenários, é necessário criar o grupo "caarha" em seu computador e certificar-se de que o grupo trabalhe com o grupo adicional.

Para instalar o mecanismo em zonas não globais no Solaris

Para zonas não globais no Solaris, você precisa executar o script *configure.sh* em cada zona não global.

Observação: para zonas não globais no Solaris 11, certifique-se de que o mecanismo do RHA seja instalado em zonas globais antes de instalá-lo em zonas não globais.

Para instalar o mecanismo em zonas não globais no Solaris

1. Execute o script *install.sh* em zonas globais como o processo superior.
2. Execute o script *configure.sh* em cada zona não global após a instalação.

Gerenciando o mecanismo

Depois da instalação, o mecanismo do CA ARCserve RHA é automaticamente gerenciado pelo sistema operacional: é iniciado durante a sequência de inicialização do sistema operacional e interrompido durante o processo de encerramento. Esses procedimentos são executados automaticamente por meio de scripts *.rc*.

Contudo, se precisar interromper manualmente o mecanismo e então reiniciá-lo, siga os procedimentos a seguir:

Linux

Para iniciar um mecanismo

```
/etc/init.d/ARCserveRHA start
```

Para interromper um mecanismo

```
/etc/init.d/ARCserveRHA stop
```

Solaris

Para iniciar um mecanismo

```
/etc/init.d/ARCserveRHA start
```

Para interromper um mecanismo

```
/etc/init.d/ARCserveRHA stop
```

AIX

Para iniciar um mecanismo

```
/opt/CA/ARCserveRHA/bin/ARCserveRHA.rc start
```

Para interromper um mecanismo

```
/opt/CA/ARCserveRHA/bin/ARCserveRHA.rc stop
```

Instalando o gerenciador

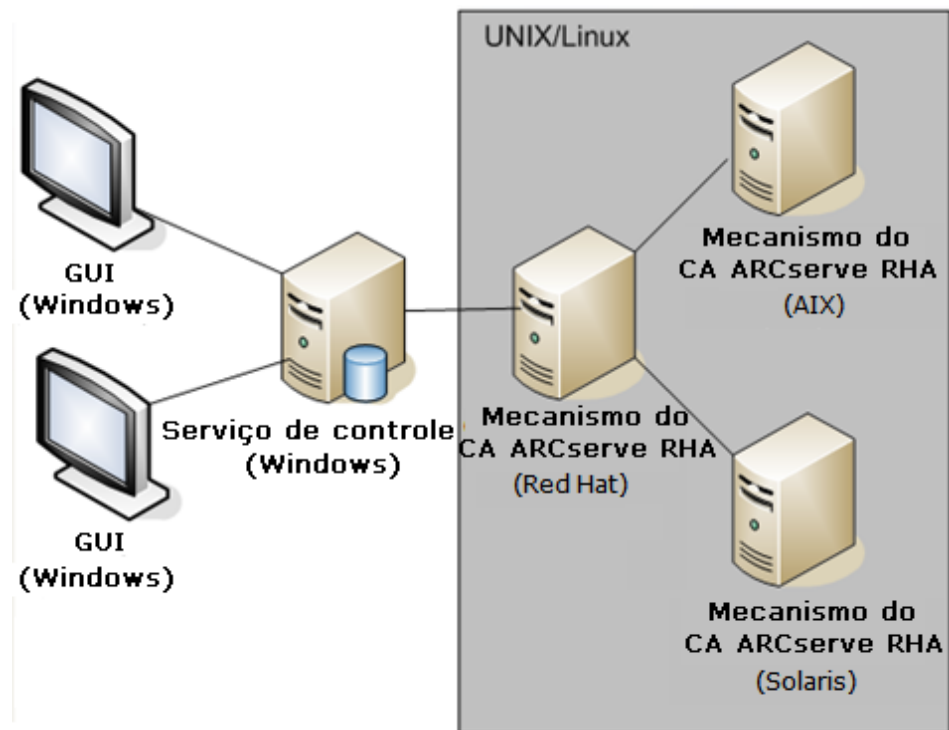
O gerenciador do CA ARCserve RHA é instalado apenas em plataformas Windows. A instalação de componentes do CA ARCserve RHA em uma plataforma Windows é muito simples e direta. O pacote de instalação contém um arquivo chamado *Setup.exe* que executa um assistente padrão MSI.

- Essa instalação (flexível) não exige reinicialização ou encerramento do aplicativo.
- O nível exigido do *instmsi.exe* é 2.0.2600.2 ou superior. Caso os requisitos mínimos não estiverem sendo atendidos, a instalação do CA ARCserve RHA atualiza automaticamente o Windows Installer para você. Entretanto, a atualização do programa de instalação exige reinicialização.

Solicitações padrão facilitam a instalação. Sua única decisão importante é em quais servidores os aplicativos deverão ser instalados (gerenciador do CA ARCserve RHA e CA ARCserve RHA PowerShell são instalados juntos):

- Instale o gerenciador do CA ARCserve RHA e o serviço de controle em qualquer computador com Windows Server que tenha acesso de rede aos computadores que você pretende gerenciar, como mostra o diagrama abaixo.
- O diretório de instalação padrão (INSTALLDIR) é: \Arquivos de programas\CA\ARCserve RHA. Todos os arquivos executáveis, DLLs e de configuração estão localizados no INSTALLDIR.
- Um usuário Windows que execute o gerenciador do CA ARCserve RHA deve ter permissão de leitura/gravação no diretório de instalação.

Instale o mecanismo do CA ARCserve RHA em todos os servidores participantes nos cenários do UNIX/Linux. Para obter mais informações sobre como instalar o gerenciador do CA ARCserve RHA, consulte o *Guia de Instalação do CA ARCserve RHA*.



Prepare o ambiente de alta disponibilidade com o script GSSnsupdate

Para executar os cenários de alta disponibilidade em domínios seguros de zona DNS, é necessário configurar o servidor UNIX ou Linux, de modo que seja possível autenticar e alterar os registros do DNS HOST A para os servidores mestre e de réplica nos cenários.

É possível configurar o ambiente UNIX/Linux do CA ARCserve RHA usando o script incluído, criado em PERL. Entre em contato com o suporte para obter outras versões deste script.

As etapas a seguir devem ser feitas em todos os hosts do UNIX/Linux em seu ambiente.

Para preparar hosts de UNIX e Linux de alta disponibilidade em domínios seguros de zona DNS

1. Configure o host do Linux como um cliente do Kerberos. Para fazer isso, edite o arquivo `/etc/krb5.conf` e faça as seguintes alterações:

```
[libdefaults]
default_realm = <nome do DOMINIO, por exemplo, XOSOFT.ORG>

[realms]
<nome do DOMINIO> = {
    kdc = <DC Server fqdn>:88
    admin_server = <DNS Server fqdn>
    default_domain = <nome do DOMINIO, por exemplo, XOSOFT.ORG>
}

[domain_realm]
. <nome do dominio>= <nome do DOMINIO>                por exemplo,
.xosoft.org =XOSOFT.ORG
```

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
default_realm = XOLAB.COM

[realms]
XOLAB.COM = {
  kdc = server01 .xolab.com:88
  admin_server = server01 .xolab.com:749
  default_domain = XOLAB.COM
}

[domain_realm]
.xolab.com = XOLAB.COM

[kdc]
profile = /var/kerberos/krb5kdc/kdc.conf
```

2. Crie um arquivo keytab com o comando ktpass no controlador de domínios especificado em "kdc" na etapa anterior. Efetue logon com uma conta de administrador do domínio no KDC.

Observação: o utilitário ktpass não pode ser carregado no Windows por padrão. É possível obtê-lo a partir do pacote Ferramentas de Suporte do Windows.

ktpass -princ host/<nome@DOMAIN> -mapuser <administrador do domínio@DOMAIN> -pass <senha> -out c:\ <nome do arquivo>.keytab -ptype KRB5_NT_PRINCIPAL

```
C:\>ktpass -princ host/xodemo@XOLAB.COM -mapuser testuser@XOLAB.COM -pass gazwsx
-out C:\xodemo.keytab -ptype KRB5_NT_PRINCIPAL
Targeting domain controller: calabdc01.xolab.com
Successfully mapped host/xodemo to testuser.
Key created.
Output keytab to C:\xodemo.keytab:
Keytab version: 0x502
keysize 48 host/xodemo@XOLAB.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 4 etype 0x3 (DES-CBC-MD5) keylength 8 (0x8545b3195d835497)
Account testuser has been set for DES-only encryption.
C:\>
```

3. Transfira o arquivo keytab <nome do arquivo>.keytab para o host do Linux com segurança.
4. No host do Linux, combine o arquivo keytab em um único arquivo denominado /etc/krb5.keytab usando o programa ktutil. Talvez seja necessário instalar o pacote ktutil primeiro.

```
[root@server01-1x1 bin]# ktutil

ktutil: rkt /root/ <nome do arquivo>.keytab

ktutil: wkt /etc/krb5.keytab

ktutil: list

ktutil: q
```

```
[root@server01 ~]# /usr/kerberos/sbin/ktutil
ktutil: rkt ./xodemo.keytab
ktutil: wkt /etc/krb5.keytab
ktutil: list
slot KVNO Principal
-----
1 5 host/test@XOLAB.COM
ktutil: q
[root@calabrsrv07-1x1 ~]#
```

5. Verifique se o horário do Linux está sincronizado com o servidor NTP ou com o servidor Microsoft DNS.
6. Copie o script PERL do arquivo nsupdate-gss.pl e instale o conjunto de bibliotecas PERL necessárias a ele. Essas fontes de PERL podem ser encontradas no site <http://search.cpan.org> ou em outro RPM.

```
perl-Digest-HMAC
perl-Net-IP
perl-Net-DNS
perl-GSSAPI
perl-Krb5...
```

7. Altere o nome principal do arquivo keytab do Kerberos no script nsupdate-gss.pl localizado em /opt/CA/ARCserve RHA/ para que seja compatível com o nome escolhido acima, por exemplo, host/xodemo.

```
#####
my $sys_retcode = system("kinit -k host/xodemo");
if ($sys_retcode != 0) {
    print "Failt to create and cache Kerberos ticket through 'kinit'\n";
    exit 1;
}
#####
```

8. Execute o seguinte teste para garantir que o ambiente esteja pronto, e que o script possa atualizar os registros do DNS A com segurança.

```
./nsupdate-gss.pl 192.168.88.1 shagu01-RHEL5u3-x64 xosoft.org --
add_ips=192.168.88.21 --ttl=60 --del_ips=192.168.88.31
```

9. Defina o script nsupdate-gss.pl script no arquivo ws_rep.cfg localizado no diretório de instalação /opt/CA/ARCserveRHA/bin para executar uma atualização segura com o Microsoft DNS. Remova o # da frente da linha "GSSnupdateScript =" como mostrado a seguir.

```
#####
# Script para fazer a atualização segura de maneira dinâmica no servidor MS
DNS em hosts do UNIX/Linux
GSSnupdateScript = "[INSTALLDIR]/scripts/nsupdate-gss.pl"
#
# O usuário pode solicitar suporte para obter ajuda em http://support.ca.com/
ou
# definir o script pelo shell ou PERL com os argumentos correspondentes
# GSSnupdateScript NAME_SERVER HOST DOMAIN [options]
```



```
# Opções:  
#      --add_ips=IPS      IPs de destino para registros A a serem  
adicionados  
#      --ttl=TTL         TTL para a adição de registros A  
#      --del_ips=IPS      IPs de destino para registros A a serem  
removidos
```

10. Interrompa e reinicie o mecanismo:

```
/etc/init.d/ARCserveRHA stop  
  
/etc/init.d/ARCserveRHA start
```

11. Repita esse procedimento para o outro host.

Atualizando o CA ARCserve RHA

Considere o seguinte, antes de atualizar para esta release:

- Interrompa os cenários em execução.
- Não é necessário desinstalar manualmente a versão anterior. O processo de instalação remove automaticamente a versão anterior.
- Copie cenários antigos no computador que está executando esta versão da GUI de gerenciamento do CA ARCserve RHA. Depois de copiados, você pode importá-los para esta versão do CA ARCserve RHA usando a seleção no menu Cenário, Importar. Os cenários podem estar localizados em:
 - UNIX: /opt/CA/ARCserveRHA/bin/ws_scenarios
 - Windows: Arquivos de programas (x86)/CA/ARCserve RHA/Gerenciador/ws_scenarios

Desinstalando o CA ARCserve RHA

Antes de desinstalar o CA ARCserve RHA, é preciso interromper todos os cenários em execução e verificar se há algum diretório montado pelo xofs.

Para verificar a existência de diretórios montados pelo xofs, certifique-se de que o arquivo /etc/xofs_mnttab esteja vazio. Se ele não estiver vazio, consulte *Descarregar drivers do xofs* (na página 37).

Observação: você pode ignorar o processo de verificação; basta reinicializar o computador ao final do procedimento de desinstalação.

Desinstalar o CA ARCserve RHA

O procedimento a seguir pode ser usado para desinstalar o CA ARCserve RHA de todas as plataformas UNIX e Linux suportadas.

Para desinstalar o CA ARCserve RHA

1. Torne-se um "superusuário".
2. Certifique-se de que todos os cenários de replicação tenham sido interrompidos.
3. Execute o seguinte script de desinstalação:

```
/opt/CA/ARCserveRHA/bin/uninstall.sh
```

Você será solicitado a confirmar o procedimento de desinstalação. Por exemplo: *Desinstalar o CA ARCserve RHA (y/n)*

4. Digite y e pressione Enter.
5. [Opcional] Reinicialize.

Capítulo 3: Métodos de redirecionamento

O CA ARCserve High Availability (CA ARCserve HA) monitora todos os eventos críticos, incluindo falha global do servidor e todas as falhas do serviço de banco de dados, e inicia uma alternância de forma automática ou por meio do acionamento de um botão.

Quando o servidor mestre fica indisponível, suas atividades podem ser alternadas automaticamente para um local remoto (réplica). A alternância, que é transparente para o usuário, inclui o início imediato de um banco de dados sincronizado em espera e o redirecionamento de todos os usuários para esse banco de dados em um tempo mínimo. Tudo isso é realizado sem exigir nova configuração de clientes ou da rede.

O redirecionamento pode ter como base os métodos a seguir:

- Mover IP (se o site em espera estiver implementado no mesmo segmento da rede)
- Redirecionar DNS, utilizado em redes locais ou quando o local remoto em espera está localizado em outra rede IP (alternância em várias redes)
- Alternar o nome do host do servidor

Observação: também podem ser aplicados scripts definidos pelo usuário para adicionar ou substituir métodos de redirecionamento incorporados. Scripts para identificar direção do tráfego de rede são necessários para oferecer suporte completo a métodos de redirecionamento personalizados ou à personalização desses métodos. Arquivos em lotes ou scripts personalizados são utilizados para identificar o servidor ativo. Esse script determina se o cenário de encaminhamento ou de retorno será executado quando o cenário for iniciado. O script é executado no mestre e na réplica: o servidor que retornar zero estará ativo. Se os dois retornarem zero, um conflito será informado.

A seleção do método de redirecionamento tem como base os requisitos do aplicativo protegido, determinados métodos podem não se aplicar a um determinado cenário. Para obter mais informações, consulte o Guia de Operações específicas do aplicativo.

Se a alternância de nome do host for usada como o método de redirecionamento nos cenários UNIX/Linux, deve-se também definir o redirecionamento de DNS.

Observação: para o método de redirecionamento Mover IP em plataformas Linux, configure o IP apenas pelo comando `ifconfig`.

Capítulo 4: Gerenciando cenários

Esta seção descreve como criar, iniciar e interromper cenários usando o gerenciador. Também é possível usar o PowerShell para gerenciar seus cenários. Para obter mais informações sobre como usar o PowerShell para criar um cenário, consulte o *Guia do CA ARCserve RHA PowerShell*.

Importante: O CA ARCserve RHA é o mais adequado para a replicação de arquivos de dados. Não é recomendável replicar arquivos executáveis e bibliotecas, pois isso pode impactar o desempenho do aplicativo. Durante a criação do cenário, você pode excluir esses arquivos da replicação.

A partir desta release, você pode usar os cenários de alta disponibilidade para proteger seu ambiente UNIX.

Esta seção contém os seguintes tópicos:

[Criar um cenário de replicação do UNIX](#) (na página 22)

[Para criar um cenário de alta disponibilidade do UNIX](#) (na página 26)

[Iniciar um cenário](#) (na página 28)

[Interromper um cenário](#) (na página 30)

[Considerações sobre o cenário no UNIX/Linux](#) (na página 31)

Criar um cenário de replicação do UNIX

A proteção de computadores UNIX e Linux usando o CA ARCserve RHA exige cenários que identifiquem os servidores mestre e de réplica, assim como as propriedades que controlam o comportamento do cenário. Você pode criar cenários de servidor de arquivos ou do Oracle, conforme necessário. A detecção automática é usada para proteger somente uma sessão do Oracle in um cenário. Se mais de uma sessão do Oracle deve ser protegida em um cenário, use o tipo de cenário de servidor de arquivos. A criação do cenário é um processo com a ajuda de um assistente e as etapas para a criação de cenários de servidor de arquivos e do Oracle são bastante parecidos. Onde há diferenças, elas são evidentes. Para obter instruções detalhadas, consulte o Guia de Operações adequado.

Observação: não pode ocorrer intersecção de diretórios raiz em diferentes cenários, isto é, não é possível criar um segundo cenário de replicação usando o mesmo diretório mestre e raiz usados para seu primeiro cenário de replicação.

Use seu navegador web para conectar-se ao CA ARCserve RHA usando o serviço de controle, efetue logon na página do portal e execute a GUI de gerenciamento. Se essa for a primeira vez que você está executando a GUI, ela é automaticamente instalada usando a tecnologia ClickOnce™. O URL da página do porta é o seguinte:

`http://<ControlServiceHost>:8088/entry_point.aspx`

1. Selecione Cenário e Novo, no gerenciador, ou clique no botão Novo cenário na barra de ferramentas.
O Assistente de criação de cenários é exibido.
2. Selecione Criar novo cenário e clique em Avançar.
A caixa de diálogo Selecionar o tipo de servidor e de produto é aberta.
3. Selecione as opções de cenário necessárias, da seguinte forma:
 - a. Na lista Selecionar tipo de cenário, selecione o tipo de cenário a ser criado. Para replicação em UNIX/Linux, somente cenários de servidor de arquivos e Oracle são suportados.
 - b. Nas opções Selecionar o tipo de produto, selecione Cenário de replicação e de recuperação de dados (DR).
4. Clique em Avançar.
A caixa de diálogo Hosts mestre e de réplica é aberta.

5. Digite os nomes ou os IPs dos servidores mestre e de réplica que deseja proteger e clique em Avançar.

A caixa de diálogo Verificação do mecanismo é aberta. Aguarde enquanto o status da versão do mecanismo é verificado. Se a versão atual estiver desatualizada, o CA ARCserve RHA perguntará se deseja atualizá-la agora. Você pode instalar a versão mais recente ou continuar. Quando a verificação estiver concluída, clique em Avançar.

Observação: se o tipo de cenário for Oracle, serão solicitadas as credenciais de usuário. Digite as credenciais de uma conta com privilégios administrativos no banco de dados de modo que o CA ARCserve RHA possa consultar a configuração do Oracle no servidor mestre.

6. Digite o nome da sessão do Oracle, o administrador do banco de dados do Oracle e o nome de usuário/senha e, em seguida, clique em OK.
 - Nos cenários do **servidor de arquivos**, a caixa de diálogo Diretórios raiz do mestre é aberta. Selecione os arquivos e/ou diretórios a serem replicados a partir do mestre e clique em Avançar para continuar até a tela Diretórios raiz da réplica.
 - Nos cenários do **Oracle**, a caixa de diálogo Selecionar espaços de tabela para replicação é aberta no lugar da caixa de diálogo Diretórios raiz do mestre. O CA ARCserve RHA fornece uma lista de resultados detectados automaticamente no servidor mestre. Selecione ou desmarque os bancos de dados para replicação, conforme necessário e ative a opção Replicar novos arquivos criados pelo usuário nos diretórios raiz listados. Clique em Avançar para continuar até a tela Diretórios raiz da réplica.

A caixa de diálogo Diretórios raiz da réplica é aberta. Dependendo do tipo de cenário que está criando, a caixa de diálogo Diretórios raiz da réplica mostrará uma lista de diretórios para o banco de dados do Oracle ou do servidor de arquivos.

7. Selecione os arquivos e/ou os diretórios na réplica em que deseja armazenar os dados a serem replicados e clique em Avançar.

Observação: se a mesma estrutura de diretório existir no servidor de réplica, o assistente a selecionará automaticamente como o diretório que receberá a replicação.

A caixa de diálogo Propriedades do cenário é aberta.

8. Configure as propriedades do mestre e de réplica. Normalmente, os valores padrão são adequados. É possível modificar todas as configurações deste painel depois que o cenário estiver criado.

Observação: o spool é uma pasta em um disco no qual são armazenados temporariamente (ou seja, colocados em spool) dados a serem replicados. Os parâmetros do spool, localizados na guia Propriedades (no mestre e na réplica) ou definidos com o Assistente de criação de cenários, determinam quanto espaço em disco ficará disponível para spool. Na maioria dos casos, os valores padrão são suficientes. Porém, se decidir alterá-los, use valores no mínimo iguais a 10% do tamanho total do conjunto de dados. Consulte o *Guia de Administração do CA ARCserve RHA* para obter mais informações.

A caixa de diálogo Propriedades do mestre e da réplica é aberta.

9. Defina a opção Retrocesso de dados como *Ativado*, no painel Propriedades da réplica, caso deseje ativar a recuperação de dados perdidos a partir da réplica usando pontos de retrocesso. Para obter mais informações sobre o uso do retrocesso de dados, consulte o tópico Retrocesso de dados.
10. Quando estiver satisfeito com as propriedades do mestre e da réplica, clique em Avançar.

A caixa de diálogo Verificação do cenário é exibida e o assistente verifica sua configuração.

11. Se tiver sido verificado com êxito, clique em Avançar, caso contrário, se ocorrerem erros, clique no botão Voltar e corrija as configurações do cenário.

Depois da verificação do cenário, a página Execução do cenário é exibida e a execução do cenário é solicitada. A execução do cenário inicia o processo de sincronização dos dados.

12. Clique em Executar agora para iniciar o cenário ou clique em Concluir para encerrar a criação do cenário e executá-lo posteriormente.

O processo de sincronização é iniciado.

Para zonas não globais no Solaris

Criar vários cenários na zona global e gerenciar todos os cenários a partir de lá. A maioria das etapas são as mesmas, exceto o seguinte:

1. Digite o endereço IP da zona global como o endereço IP principal.
2. Use os comandos a seguir para obter as informações sobre o diretório de raiz da zona e sobre a zona:

```
/usr/sbin/zoneadm list -vi  
zonecfg -z <zonenname> info
```

3. Ao definir o diretório raiz, adicione manualmente o diretório raiz da zona não global no caminho que deseja proteger. Nesse caso, não é possível usar a detecção automática para aplicativos como Oracle.

Para criar um cenário de alta disponibilidade do UNIX

Criar cenários de alta disponibilidade do UNIX, do mesmo modo que para qualquer outro cenário de alta disponibilidade, usando o Assistente de criação de cenários.

Para obter informações sobre a criação de um cenário de alta disponibilidade para um banco de dados Oracle, consulte o *Guia de Operações do CA ARCserve RHA para Oracle*.

Para criar um novo cenário HA de UNIX

1. Inicie o gerenciador do CA ARCserve RHA. Selecione Arquivo, Criar, Novo cenário ou clique no botão Novo cenário.

A caixa de diálogo Bem-vindo é aberta.

2. Clique em Criar cenário e digite um Nome do grupo de cenários ou selecione um da lista e clique em Avançar.

A caixa de diálogo Selecionar o tipo de servidor e de produto é aberta.

3. Selecione o servidor de arquivos e certifique-se de que o tipo de produto para o cenário de alta disponibilidade está selecionado. Para tarefas na réplica, selecione Nenhum e, em seguida, clique em Avançar.

A caixa de diálogo Hosts mestre e de réplica é aberta.

4. Digite o nome de um cenário, digite o Nome do host ou Endereço IP e o Número da porta para os servidores mestre e de réplica, ative a opção Verificar o mecanismo do CA ARCserve RHA nos hosts e clique em Avançar. É possível que as credenciais do usuário sejam solicitadas. Se forem, digite as credenciais apropriadas e clique em OK.

A caixa de diálogo Verificação do mecanismo é exibida, se o mecanismo de verificação tiver sido ativado.

5. Aguarde a conclusão da verificação e clique em Avançar para continuar, quando estiver concluída.

A caixa de diálogo Diretórios raiz do mestre é exibida, mostrando a lista de diretórios identificados no mestre.

6. Clique em Avançar.

A tela Diretórios raiz da réplica é aberta.

7. Defina as propriedades da réplica e clique em Avançar.

A tela Propriedades do cenário é exibida.

8. Configure as propriedades necessárias e clique em Avançar. Para obter mais informações sobre como configurar propriedades do cenário, consulte o *Guia de Administração do CA ARCserve RHA*.

A tela Propriedades do mestre e da réplica é exibida.

9. Configure as propriedades necessárias e clique em Avançar. Para obter mais informações sobre como configurar propriedades do mestre e da réplica, consulte o *Guia de Administração do CA ARCserve RHA*.

A tela Propriedades de alternância é aberta.

10. Configure as propriedades de alternância e clique em Avançar.

Observação: os valores padrão recomendados já estão definidos. Para obter mais informações sobre como configurar propriedades de alternância, consulte o *Guia de Administração do CA ARCserve RHA*.

1. A caixa de diálogo Início da alternância e da replicação inversa é aberta.

11. Faça as seleções necessárias para as opções conforme abaixo, para controle automático de alternância e replicação inversa, em seguida, clique em Avançar.

Início da alternância

Especifica se deve iniciar uma alternância de maneira automática ou manual. A alternância automática é iniciada quando o servidor mestre estiver desativado ou uma falha de banco de dados for detectada. A alternância manual é iniciada pelo administrador. Em ambos os casos, uma mensagem é exibida quando uma falha for detectada.

Início da replicação inversa

Especifica se deve iniciar uma alternância reversa de maneira automática ou manual. Depois de uma alternância, o cenário é interrompido e a replicação reversa é iniciada.

Observação: não é recomendável **não** definir essas opções como automáticas em um ambiente de produção.

A tela Verificação do cenário é aberta.

12. Aguarde enquanto o processo de Verificação do cenário é concluído.

Se a Verificação do cenário listar algum erro, será necessário resolvê-lo para poder continuar. Se algum aviso for listado, você também deverá resolvê-lo para poder continuar com êxito. Após fazer as alterações, clique em Repetir para repetir a verificação.

13. Clique em Avançar.

A caixa de diálogo Execução do cenário é aberta.

14. Clique em Executar agora para iniciar a sincronização e ativar o cenário. Clique em Concluir para executar o cenário posteriormente.

Para zonas não globais no Solaris

Criar vários cenários na zona global e gerenciar todos os cenários a partir de lá. A maioria das etapas são as mesmas, exceto o seguinte:

1. Digite o endereço IP da zona global como o endereço IP principal.
2. Use os comandos a seguir para obter as informações sobre o diretório de raiz da zona e sobre a zona:


```
/usr/sbin/zoneadm list -vi  
zonecfg -z <zonename> info
```

3. Ao definir o diretório raiz, adicione manualmente o diretório raiz da zona não global no caminho que deseja proteger. Nesse caso, não é possível usar a detecção automática para aplicativos como Oracle.

Iniciar um cenário

É possível iniciar um cenário usando o gerenciador.

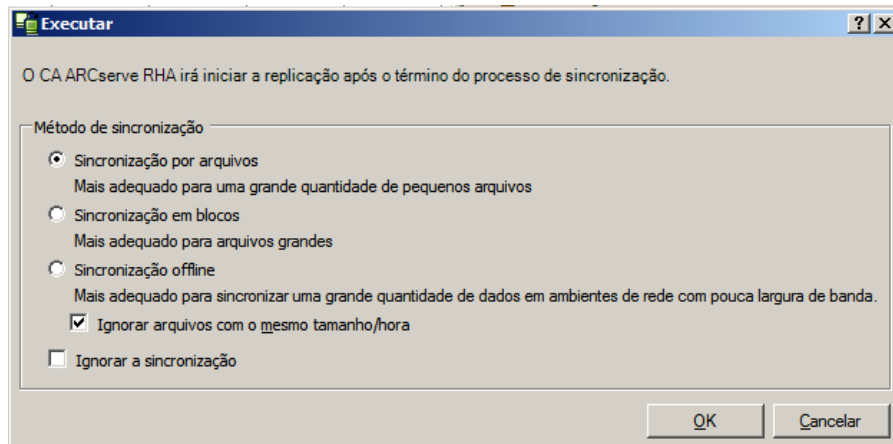
Para iniciar um cenário

1. Selecione o cenário que deseja executar no painel Cenário.
2. Clique em Executar  na barra de ferramentas.

Uma caixa de diálogo com os resultados da verificação é aberta, solicitando sua aprovação para a execução do cenário.

3. Clique em Executar. Use o botão Avançado para exibir detalhes do cenário do mestre e da réplica.

A caixa de diálogo Executar é aberta.



Observação: ao iniciar cenários com base em UNIX, você pode ignorar a sincronização em nível de arquivo e bloco.

4. Selecione Sincronização de arquivos e clique em OK.

Observação: se estiver executando um cenário do servidor Oracle, desmarque a caixa de seleção Ignorar arquivos de mesmo tamanho/hora e selecione Sincronização em blocos.

O gerenciador agora indica que o cenário está em execução, por meio de um símbolo verde localizado à esquerda do cenário:

Novo grupo						
Cenário	Estado	Produto	Servidor	Modo		
FileServer 1	Em execução	HA/AR	FileServer	Online		
Hosts	Alterado	Dados envi...	Arquivos e...	Dados rece...	Arquivos r...	No spool
155.35.75.141	0,00 Bytes	0,00 Bytes	0	-	-	0,00 Bytes
155.35.75.160						

Quando um cenário está em execução, uma guia de estatísticas é exibida (na parte inferior do painel da extrema direita):



Além disso, um relatório é gerado por padrão quando a sincronização ocorre.

Interromper um cenário

É possível interromper um cenário usando o gerenciador.

Para interromper um cenário:

1. Clique no botão Interromper  na barra de ferramentas.

É exibida uma mensagem de confirmação, solicitando que você aprove a interrupção do cenário.

2. Clique em Sim.

O cenário é interrompido.

Observação: depois de interromper o cenário, você verá que o gerenciador não mostrará mais o símbolo verde à esquerda do cenário e que a guia de estatísticas não estará mais disponível.

Considerações sobre o cenário no UNIX/Linux

Considere o seguinte ao criar cenários no UNIX/Linux:

- Um diretório pode estar presente em apenas um cenário
- No NFS (Network File Sharing), V4 não é suportado. Você deve instalar o mecanismo no servidor NFS e verificar se o diretório exportado reside no diretório raiz.
- O suporte a NFS não é fornecido com o SUSE 11.
- No caso da replicação Windows para UNIX, Windows ACLs são perdidos.
- Na replicação UNIX para Windows, UID, GUID, links simbólicos e links físicos são perdidos.
- Nomes de arquivos no Windows não são sensíveis a maiúsculas e minúsculas, portanto é possível que haja conflito.
- Não pode ocorrer intersecção de diretórios raiz em diferentes cenários, isto é, não é possível criar um segundo cenário de replicação usando o mesmo diretório mestre e raiz usados para seu primeiro cenário de replicação.
- Parâmetros de alta disponibilidade em um host UNIX/Linux:
 - Informações do sistema: o controlador de domínio do AD e as propriedades de cluster da MS não são suportados, portanto os valores serão sempre definidos como *Não*. Para a propriedade do servidor DNS, somente o processo *nomeado* do servidor BIND é verificado; se o *nomeado* estiver em execução, a propriedade do servidor DNS é definida como *Sim*, caso contrário, será definida como *Não*.
 - Configuração de rede: o nome NetBIOS não é suportado.
- Os links físicos agora são suportados. Os links físicos não podem ser criados entre diferentes sistemas de arquivos ou diretórios raiz no mesmo sistema de arquivos.
- Não há suporte à execução simultânea de cenários de diferentes zonas não globais no Solaris. A solução alternativa é criar diversos cenários a partir da zona global do Solaris e gerenciar todos os cenários a partir daí.

Observação: certifique-se de que todas as pastas em zonas locais estejam acessíveis a partir da zona global do Solaris.

Apêndice A: Arquivos instalados

Durante a instalação do CA ARCserve RHA, diferentes arquivos são instalados para sistemas operacionais distintos, conforme descrevem as próximas seções.

Esta seção contém os seguintes tópicos:

[Arquivos instalados no Red Hat e Novell SUSE Linux Enterprise](#) (na página 33)

[Arquivos instalados no IBM AIX](#) (na página 34)

[Arquivos instalados no Solaris](#) (na página 35)

Arquivos instalados no Red Hat e Novell SUSE Linux Enterprise

Em plataformas Linux, são instalados estes arquivos:

Arquivo instalado	Descrição
/opt/CA/ARCserveRHA/bin/ws_rep	O mecanismo do CA ARCserve RHA opera como daemon no modo de usuário. Sua principal responsabilidade é colaborar com o módulo de kernel xofs (filtrando o sistema de arquivos), para acompanhar as alterações do sistema de arquivos e propagá-las no cenário da réplica.
/opt/CA/ARCserveRHA/kernel/fs/xofs.*	Um sistema de arquivos proprietário - <i>xofs</i> . Implementado na forma de um módulo de kernel que pode ser carregado. O objetivo principal do xofs é acompanhar as alterações do sistema de arquivos e notificá-las ao mecanismo. Carregado durante a inicialização do sistema (com /etc/init.d/CA ARCserve RHA). Observação: <i>.up</i> se destina a uniprocessor e <i>smp</i> a vários processadores simétricos.
/etc/init.d/ARCserveRHA	Script de inicialização utilizado para iniciar e encerrar o mecanismo.
/etc/pam.d/ws_rep	Necessário para o CA ARCserve RHA autenticar conexões de gerenciamento na interface gráfica do usuário.
/opt/CA/ARCserveRHA/bin/README	Arquivo Leiamme do CA ARCserve RHA
/opt/CA/ARCserveRHA/bin/ws_rep.cfg	Arquivo de configuração do CA ARCserve RHA

/opt/CA/ARCserveRHA/bin/uninstall.sh Desinstala o software.

Arquivos instalados no IBM AIX

Em plataformas AIX, são instalados estes arquivos:

Arquivo instalado	Descrição
/opt/CA/ARCserveRHA/bin/ws_rep	O mecanismo do CA ARCserve RHA opera como daemon no modo de usuário. Sua principal responsabilidade é colaborar com o módulo de kernel xofs (filtrando o sistema de arquivos), para acompanhar as alterações do sistema de arquivos e propagá-las no cenário da réplica.
/opt/CA/ARCserveRHA/bin/xofs.ext	Um sistema de arquivos proprietário - <i>xofs</i> . Implementado na forma de uma extensão de kernel que pode ser carregada. O objetivo principal do xofs é acompanhar as alterações do sistema de arquivos e notificá-las ao mecanismo. Carregado durante a inicialização do sistema (com /opt/CA/ARCserveRHA/bin/ARCserveRHA.rc).
/opt/CA/ARCserveRHA/bin/xoctl	Utilitário auxiliar (auxiliar do sistema de arquivos). Carrega xofs previamente durante a inicialização do sistema.
/opt/CA/ARCserveRHA/bin/xoumount	Utilitário auxiliar (<i>umount xofs</i>). Análogo do utilitário padrão da linha de comando <i>umount</i> . Observação: o comando padrão <i>umount</i> não funcionará para xofs na release atual do CA ARCserve RHA.
/opt/CA/ARCserveRHA/bin/ARCserveRHA.rc	Script de inicialização utilizado para iniciar e encerrar o mecanismo.
/opt/CA/ARCserveRHA/bin/uninstall.sh	Desinstala o software.

Arquivos instalados no Solaris

Em plataformas Solaris, são instalados estes arquivos:

Arquivo instalado	Descrição
/opt/CA/ARCserveRHA/bin/ws_rep	O mecanismo do CA ARCserve RHA opera como daemon no modo de usuário. Sua principal responsabilidade é colaborar com o módulo de kernel xofs (filtrando o sistema de arquivos), para acompanhar as alterações do sistema de arquivos e propagá-las no cenário da réplica.
/usr/kernel/fs/xofs e /usr/kernel/fs/sparcv9/xofs	Um sistema de arquivos proprietário - <i>xofs</i> . Implementado na forma de um módulo de kernel que pode ser carregado. O objetivo principal do xofs é acompanhar as alterações do sistema de arquivos e notificá-las ao mecanismo. Carregado sob demanda durante a inicialização do cenário de replicação.
/opt/CA/ARCserveRHA/bin/uninstall.sh	Desinstala o software.
/opt/CA/ARCserveRHA/bin/configure.sh (zonas)	Configura ws_rep em zonas não globais.

Apêndice B: Solução de problemas

As informações a seguir ajudam a solucionar problemas nos cenários do CA ARCserve RHA para UNIX/Linux:

- Esta versão do CA ARCserve RHA oferece um recurso "uninject" que permite que o xofs descarregue automaticamente, mesmo quando há alguns arquivos abertos durante uma operação de interrupção de um cenário.

Esta seção contém os seguintes tópicos:

[Descarregar drivers do xofs](#) (na página 37)

Descarregar drivers do xofs

Se durante o procedimento de desinstalação, algum dos diretórios for acidentalmente deixado sob o controle do xofs (por exemplo, o cenário estava em execução e o diretório havia sido montado pelo xofs), o procedimento de desinstalação não poderá descarregar o driver do xofs do sistema.

Nesse caso, basta reinicializar o computador ou descarregar o driver do xofs manualmente.

Para descarregar os drivers do xofs

1. Verifique se há algum ponto de montagem de xofs usando o seguinte comando:

```
#cat /etc/xofs_mnttab
```

2. Interrompa todos os processos mantidos no diretório. Use o comando *fuser* apropriado para sua plataforma para detectar processos que tenham open files em seu diretório:

AIX e Solaris

```
#fuser -c <dir_from_xofs_mnttab>
```

Linux

```
#fuser -u <dir_from_xofs_mnttab>
```

3. Use o comando `umount` para o diretório detectado na etapa 1.

```
#umount <dir_from_xofs_mnttab>
```

4. Verifique se algum processo está usando o driver do xofs e descarregue-o manualmente. Siga as instruções para sua plataforma:

AIX

Execute como raiz o seguinte comando para verificar se o xofs está carregado no kernel:

```
echo lke | kdb| grep xofs
```

Execute como raiz o seguinte comando para descarregar o driver do xofs:

```
/opt/CA/ARCserveRHA/bin/xoctl u /opt/CA/ARCserveRHA/bin/xofs.ext
```

Solaris

Execute o seguinte comando para verificar se o driver está carregado na memória:

```
modinfo|grep xofs
```

Execute o seguinte comando para descarregar o driver do xofs:

```
modunload -i <xofs ID>
```

Linux

Execute o seguinte comando para verificar se o contador de referência do driver do xofs é 0:

```
/sbin/lsmmod|grep xofs
```

Execute o seguinte comando para descarregar o driver do xofs:

```
/sbin/rmmod xofs
```

Índice remissivo

A

- arquivos instalados
 - em IBM AIX - 34
 - em Red Hat e Novell SUSE Linux Enterprise - 33
 - em Solaris - 35

C

- cenários
 - criação - 22, 26
 - execução - 28
 - interrupção - 30
 - propriedades de - 22

D

- descarregar driver do xofs - 37

G

- Gerenciador do CA ARCserve RHA
 - criando um cenário de alta disponibilidade em UNIX - 26
 - criando um cenário em UNIX - 22
 - iniciando um cenário - 28
 - instalando - 12
- gerenciando o mecanismo do CA ARCserve RHA - 11

I

- instalando
 - Gerenciador do CA ARCserve RHA - 12
 - Mecanismo do CA ARCserve RHA - 10, 11

M

- Mecanismo do CA ARCserve RHA, instalando - 10

R

- relatórios - 28, 30
- replicação e recuperação de dados, definindo para cenário - 22

- retrocesso de dados
 - ativando opção - 22

S

- servidor de réplica
 - definição - 22

U

- UNIX, versões suportadas - 7

V

- versões suportadas - 7