Guia do Usuário do Agente do Arcserve® Unified Data Protection para Linux

Versão 8.x

arcserve®

Conteúdo

Entre em contato com o Suporte da Arcserve

A equipe do Suporte da Arcserve oferece uma ampla gama de recursos para solucionar seus problemas técnicos e fornece acesso fácil a informações importantes sobre o produto.

Entrar em contato com o suporte

Com o Suporte da Arcserve:

- É possível ter contato direto com a mesma biblioteca de informações compartilhada internamente por nossos especialistas do Suporte da Arcserve. Este site fornece acesso aos documentos de nossa base de conhecimento. A partir daqui, é fácil pesquisar e localizar os artigos da base de conhecimento relacionados ao produto que contêm soluções testadas em campo para muitos dos problemas principais e comuns.
- Você pode usar nosso link para o Bate-papo ao vivo para iniciar instantaneamente uma conversa em tempo real entre você e a equipe do Suporte da Arcserve. Com o Bate-papo ao vivo, você poderá obter respostas imediatas para suas dúvidas e preocupações, sem deixar de manter o acesso ao produto.
- É possível participar da Comunidade global de usuários da Arcserve para fazer perguntas e responder a perguntas de outros usuários, compartilhar dicas e truques, discutir práticas recomendadas e iniciar conversas com colegas.
- É possível abrir um ticket de suporte. Ao abrir um ticket de suporte online, é possível esperar um retorno de chamada de um de nossos especialistas na área do produto sobre o qual está perguntando.
- Você pode acessar outros recursos úteis adequados ao seu produto da Arcserve.

Capítulo 1: Entendendo o Agente do Arcserve UDP (Linux)

Esta seção contém os seguintes tópicos:

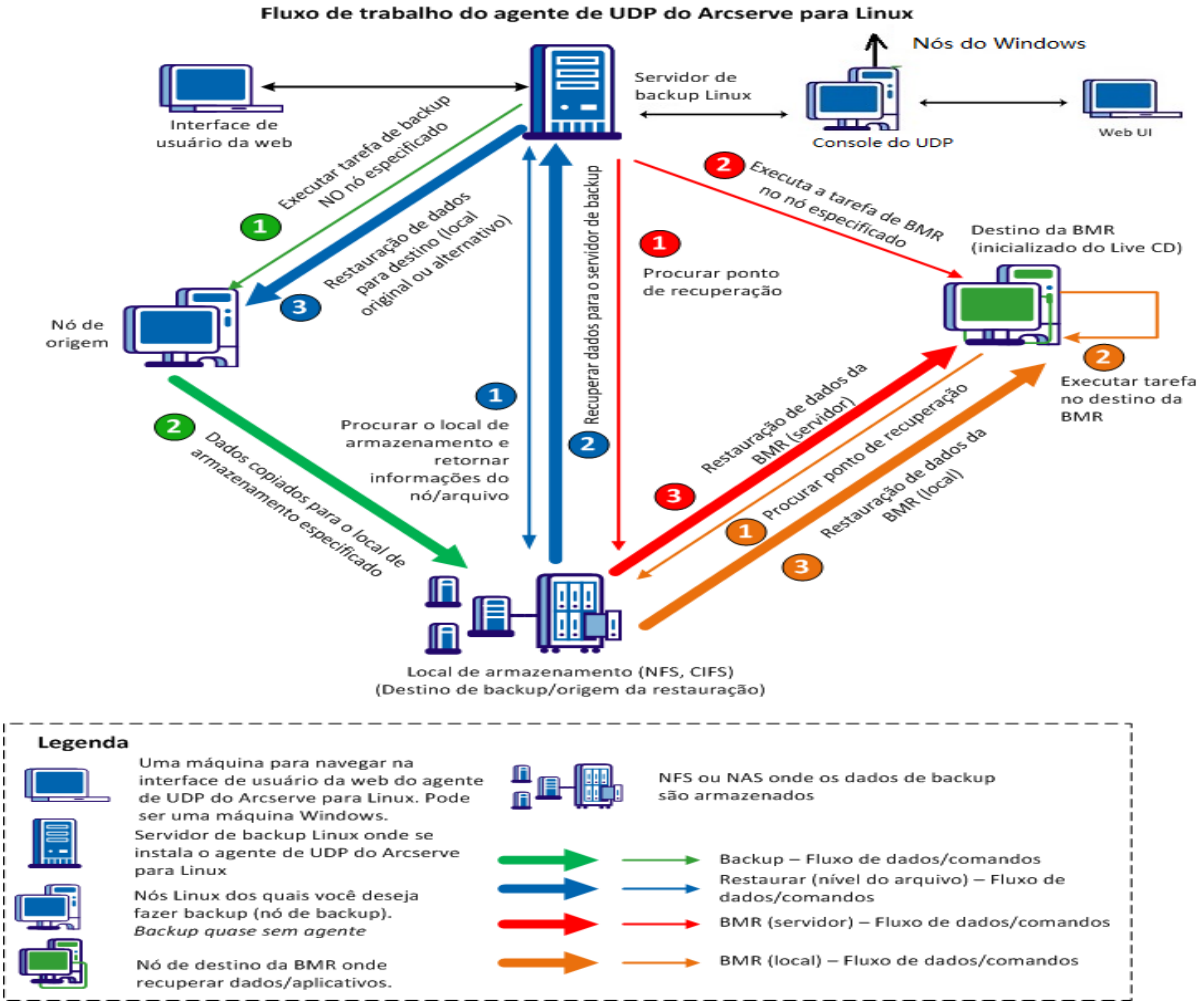
Introdução

O Arcserve UDP para Linux (Agente do Arcserve UDP (Linux)) é um produto de backup com base em disco criado para sistemas operacionais Linux. Ele oferece uma maneira rápida, simples e confiável de proteger e recuperar informações comerciais essenciais. O Agente do Arcserve UDP (Linux) controla as alterações em um nó no nível de bloco e, em seguida, faz backup somente dos blocos alterados em um processo incremental. Como resultado, o Agente do Arcserve UDP (Linux) permite executar backups frequentes, reduzindo assim o tamanho de cada backup incremental (e a janela de backup) e fornecendo um backup mais atualizado. O Agente do Arcserve UDP (Linux) também fornece o recurso de restaurar arquivos ou pastas e executar uma BMR (Bare Metal Recovery – Recuperação Bare-Metal) a partir de um único backup. É possível armazenar as informações de backup em um compartilhamento NFS (Network File System – Sistema de Arquivos da Rede), compartilhamento CIFS (Common Internet File System – Sistema Comum de Arquivos da Internet) ou no nó de origem do backup.

A BMR é o processo de restauração de um sistema de computador do estado *bare metal*. Bare metal é um computador sem sistema operacional, drivers e aplicativos de software. A restauração inclui a instalação do sistema operacional, de aplicativos de software, de drivers e, em seguida, a restauração dos dados e das configurações. A BMR é possível porque, enquanto realiza um backup de dados, o Agente do Arcserve UDP (Linux) também captura informações relacionadas ao sistema operacional, aos aplicativos instalados, aos drivers etc. Após a conclusão da BMR, o nó de destino tem o mesmo sistema operacional e dados que o nó de produção.

O Agente do Arcserve UDP (Linux) usa uma abordagem quase sem agente para permitir proteção rápida e flexível de todos os seus clientes Linux. O recurso elimina totalmente a necessidade de instalar agentes em cada nó cliente, automatizando, assim, por completo a detecção, a configuração e a proteção de todos os clientes Linux. É possível instalar o Agente do Arcserve UDP (Linux) para ajudar a proteger todo o ambiente de produção Linux. O servidor no qual você instala o Agente do Arcserve UDP (Linux) é conhecido como Servidor de backup. Após a instalação do Agente do Arcserve UDP (Linux), é possível conectar-se ao servidor de backup via rede e abrir a interface do usuário, usando um navegador.

O diagrama a seguir mostra o fluxo de trabalho geral do Agente do Arcserve UDP (Linux):


Fluxo de trabalho do agente de UDP do Arcserve para Linux
Nós do Windows
Interface de usuário da web
Servidor de backup Linux
Console do UDP
Web UI
Executar tarefa de backup NO nó especificado
Restauração de dados para destino (local original ou alternativo)
Executa a tarefa de BMR no nó especificado
Destino da BMR (inicializado do Live CD)
Procurar ponto de recuperação
Nó de origem
Recuperar dados para o servidor de backup
Procurar o local de armazenamento e retornar informações do nó/arquivo
Dados copiados para o local de armazenamento especificado
Restauração de dados da BMR (servidor)
Procurar ponto de recuperação
Restauração de dados da BMR (local)
Executar tarefa no destino da BMR
Local de armazenamento (NFS, CIFS)
(Destino de backup/origem da restauração)
Legenda
Uma máquina para navegar na interface de usuário da web do agente de UDP do Arcserve para Linux. Pode ser uma máquina Windows.
Servidor de backup Linux onde se instala o agente de UDP do Arcserve para Linux
Nós Linux dos quais você deseja fazer backup (nó de backup).
Backup quase sem agente
Nó de destino da BMR onde recuperar dados/aplicativos.
NFS ou NAS onde os dados de backup são armazenados
Backup – Fluxo de dados/comandos
Restaurar (nível do arquivo) – Fluxo de dados/comandos
BMR (servidor) – Fluxo de dados/comandos
BMR (local) – Fluxo de dados/comandos

Capítulo 2: Instalação/desinstalação do Agente do Arcserve UDP (Linux)

Esta seção contém os seguintes tópicos:

Como instalar o Agente do Arcserve UDP (Linux)

Instale o Agente do Arcserve UDP (Linux) em um servidor Linux para proteger e gerenciar todos os seus nós de origem do backup em uma IU só. Não é necessário instalar esse software nos nós de origem do backup.

Execute estas tarefas para instalar o Agente do Arcserve UDP (Linux):

- Considerações sobre a instalação
- Instalar o Agente do Arcserve UDP (Linux)
- Instalar o agente do Arcserve UDP (Linux) na nuvem AWS
- Verificar a instalação

Considerações sobre a instalação

Considere os seguintes pontos antes de iniciar a instalação:

- Quando você executa uma BMR com base em PXE (Preboot Execution Environment – Ambiente de Execução de Pré-inicialização), o servidor do Arcserve UDP para Linux e os nós de origem de produção precisam estar na mesma sub-rede. Se eles não estiverem na mesma sub-rede, certifique-se de que haja um gateway para encaminhar os pacotes de difusão do PXE nas sub-redes.
- Se o destino de backup for um servidor do NFS, verifique se o servidor do NFS oferece suporte a *bloqueio.* Também, verifique se o usuário raiz possui acesso de gravação aos nós Linux.
- Para usar um servidor do NFS como o destino do backup, instale o pacote do cliente NFS nos nós Linux.
- O perl e o sshd (Daemon de SSH) são instalados no servidor Linux e nos nós Linux que deseja fazer backup.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.
- A instalação autônoma ou silenciosa não é suportada.

Instalar o Agente do Arcserve UDP (Linux)

Instale o Agente do Arcserve UDP (Linux) em um servidor Linux para gerenciar operações de backup e restauração. Após a instalação do Agente do Arcserve UDP (Linux), é possível abrir a interface do usuário em qualquer computador usando um navegador. O servidor é referenciado como o servidor de backup.

No início da instalação, o script de instalação verifica se algum dos aplicativos obrigatórios está instalado no servidor de backup e se os aplicativos estão em execução.

Os aplicativos obrigatórios a seguir são necessários para o arquivo de instalação funcionar:

- sshd (Daemon de SSH)
- Perl

O arquivo de instalação também verifica os seguintes aplicativos opcionais no início da instalação:

- rpc.statd – esse aplicativo é usado pelo servidor NFS para implementar o bloqueio de arquivos.
- mkisofs – o Agente do Arcserve UDP (Linux) usa esse aplicativo para criar um Live CD.
- mount.nfs – o Agente do Arcserve UDP (Linux) usa esse aplicativo para montar o servidor NFS.
- mount.cifs – o Agente do Arcserve UDP (Linux) usa esse aplicativo para montar o servidor CIFS.
- ether-wake – o Agente do Arcserve UDP (Linux) usa esse aplicativo para enviar a solicitação Wake-on-LAN.

Observações:

- Certifique-se de que o servidor Linux tenha, no mínimo, 2 GB de memória. Para obter mais informações sobre os requisitos de sistema de um servidor Linux, consulte as Notas da Versão do Arcserve UDP 8.0.
- Use sudo para instalar o servidor Linux no Microsoft Azure.
- Para os sistemas Debian/Ubuntu, não é permitido à raiz efetuar logon no ssh por padrão. Para conceder ao usuário que não é raiz permissão para efetuar logon na interface do usuário do servidor de backup Linux, consulte Conceder permissões de logon aos usuários não raiz.

Siga estas etapas:

1. Efetue logon no servidor Linux como um usuário raiz.
2. Faça download do pacote de instalação do Agente do Arcserve UDP (Linux) (arquivo *.bin) na pasta raiz.

   Importante: quando você faz download do arquivo do pacote de instalação em uma pasta local, o caminho completo dessa pasta local não pode conter nenhum caractere especial, exceto espaços em branco, e só deve incluir os seguintes caracteres: a-z, A-Z, 0-9, - e _.
3. Forneça a permissão de execução para o pacote de instalação.
4. Execute o seguinte comando para iniciar a instalação:

   ./<nome_do_arquivo_de_instalação_do_linux>.bin

   O pacote de instalação verifica a plataforma suportada e exibe uma mensagem de confirmação.

   Se uma plataforma sem suporte for detectada, digite Y e pressione Enter para confirmar a instalação da plataforma sem suporte.

   Observações:

   - se um sistema operacional que não esteja em inglês for detectado, você será solicitado a selecionar o idioma aplicável antes de continuar com o processo de instalação.
   - Para oferecer suporte ao idioma coreano ao fazer a atualização de uma compilação, execute as seguintes etapas:
     a. Modifique o seguinte arquivo de configuração no servidor do agente do Arcserve UDP (Linux): */opt/Arcserve/d2dserver/nls/nls.cfg*
     b. Defina D2D_LANG= ko_KR.
     c. Reinicie o d2dserver usando o seguinte comando: *#/opt/Arcserve/d2dserver/bin/d2dserver restart*.
5. Digite Y e pressione Enter para confirmar a instalação.

   O pacote de instalação exibe as informações do contrato de licença.
6. Digite Y e pressione Enter para aceitar o contrato de licença.

   O processo de instalação do Agente do Arcserve UDP (Linux) é iniciado.

   Quando a instalação do pacote de utilitário de restauração estiver concluída, as informações de criação do Live CD são exibidas.

O Live CD é criado no seguinte local:

```
/opt/Arcserve/d2dserver/packages
```

Observação: o Live CD é necessário para se obter o endereço IP do nó de destino ao executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal).

O Agente do Arcserve UDP (Linux) é instalado e o URL de acesso ao servidor de backup Linux é exibido.

Observação: certifique-se de que as seguintes portas de entrada estejam ativadas no firewall para o servidor de backup:

- Porta TCP 22 (servidor SSH)
- Porta de difusão 67 (servidor de inicialização)
- 8014 (serviço da web do agente)
- UDP (User Datagram Protocol - Protocolo de Datagrama de Usuário), porta 69 (servidor TFTP)
- 8016 (serviço de BMR instantânea)
- 8021 (serviço de backup)

Certifique-se de que a seguinte porta de entrada esteja ativada no firewall para os nós clientes dos quais você deseja fazer backup:

- Porta TCP 22 (servidor SSH)

Certifique-se de que a porta de saída necessária para NFS, CIFS ou ambos os destinos do backup estejam ativados em seu firewall pra o servidor de backup Linux e os nós de destino da BMR.

Observação: para saber mais sobre as portas, consulte Communication Ports Used by Arcserve UDP.

7. (Opcional) Para instalar o servidor de backup Linux em uma VM no Amazon EC2 ou no Azure, siga estas etapas para criar um usuário do D2D:

   Observação: quando o servidor for iniciado, um prompt de mensagem solicitará a criação de um usuário do D2D, o qual será usado para efetuar logon na interface do usuário da web do Agente do Arcserve UDP (Linux).

   a. Digite um nome para o usuário a ser criado.

   b. Defina a senha e confirme-a digitando-a novamente.

   c. Defina se deseja que a conta do usuário seja configurada como o usuário padrão de logon para a IU da web do Agente do Arcserve UDP (Linux).

      Padrão: Y (Sim)

d. Decida após quantas falhas consecutivas de logon a conta de usuário é bloqueada.

   Padrão: 3

O Agente do Arcserve UDP (Linux) é instalado com êxito.

Instalar o Agente do Arcserve UDP (Linux) na nuvem da AWS

Assim como em uma instalação tradicional em uma máquina Linux, você pode iniciar uma instância do Agente do Arcserve UDP (Linux) diretamente usando uma AMI (Amazon Machine Image) na nuvem da AWS. Depois de iniciar a instância do Agente do Arcserve UDP (Linux), é possível abrir a interface do usuário em qualquer computador que use um navegador da web e o servidor é conhecido como o servidor de backup.

Siga estas etapas:

1. Efetue logon no console de gerenciamento do EC2 com sua conta e selecione Iniciar instância.

   O assistente para iniciar instância é exibido mostrando sete guias.

2. Na primeira guia, **Selecionar AMI**, selecione a AMI do agente do Arcserve UDP (Linux) em **AMIs da comunidade** para **Etapa 1: escolher uma AMI da Amazon** e clique em **Próximo: escolher um tipo de instância**.

   Você pode pesquisar a AMI do Agente do Arcserve UDP (Linux) usando *Arcserve_Unified_Data_Protection_Agent_Linux* em Community AMIs.

   Observação: selecione uma AMI do Agente do Arcserve UDP (Linux) com a versão mais recente para iniciar a instância.

   A segunda guia, **Escolher tipo de instância**, é exibida.

3. Selecione o tipo de instância de acordo com suas necessidades para concluir a **Etapa 2: escolher um tipo de instância** e clique em **Próximo: configurar detalhes da instância**.

   Observação: verifique se o Tipo de instância é pelo menos t2.medium e tem no mínimo 4 GB de memória. Para obter mais informações sobre os requisitos do sistema de um servidor Linux, consulte Notas da Versão do Arcserve UDP 8.0 - aprimoramentos do agente do Linux.

   A terceira guia, **Configurar instância**, é exibida.

4. Selecione os detalhes de campos como Rede, Sub-rede, IP público da atribuição automática ou não, e outros para concluir a **Etapa 3: configurar detalhes da instância**. Em seguida, clique em **Próximo: adicionar armazenamento**.

   A quarta guia, **Adicionar armazenamento**, é exibida.

5. Aloque o armazenamento para a instância para concluir a **Etapa 4: adicionar armazenamento** e clique em **Próximo: adicionar tags**.

Observação: você pode ajustar o tamanho do disco com base em suas necessidades de negócios. Verifique se o disco de instância do Linux tem um tamanho mínimo de 40 GB.

A quinta guia, **Adicionar tags** é exibida.

5. Insira as tags para a instância de destino da AMI para concluir a **Etapa 5: adicionar tags** e clique em **Próximo: configurar grupo de segurança**.

   A sexta guia, **Configurar grupos de segurança**, é exibida.

6. Execute as seguintes etapas para atribuir grupos de segurança para a instância de destino da AMI e concluir a **Etapa 6: configurar grupo de segurança**. Depois, clique em **Revisar e iniciar**:

   Siga estas etapas:

   a. Crie um grupo de segurança para SSH e Agente do Arcserve UDP (Linux).

   b. Verifique se **Tipo** *SSH* está ativado na porta 22 e configure **Origem** como *Qualquer lugar*.

   c. Verifique se *Regra TCP personalizada* está ativada em **Tipo** na porta 8014 usada pelo tomcat e configure **Origem** como *Qualquer lugar*.

   d. Verifique se a porta 8016 usada pelo d2ddss e a porta 8021 usada pelo cresvc estão com a Regra TCP personalizada ativada em **Tipo** e configure **Origem** da regra como Personalizada.

      Observação: você pode especificar a origem personalizada com o formato CIDR para permitir que o d2ddss auxilie as instâncias do Linux que estejam na mesma sub-rede com o Agente do Arcserve UDP (Linux), mas fique inacessível a outras máquinas da internet. Por exemplo, se a sub-rede CIDR for 102.31.16.0/20, você também pode especificar a origem como 102.31.16.0/20.

   A sétima guia, **Revisão**, é exibida.

7. Verifique os detalhes selecionando ou criando um par de chaves para se conectar à instância e concluir a **Etapa 7: revisar inicialização da instância**. Em seguida, clique em **Iniciar instância**.

8. Na instância iniciada do Agente do Arcserve UDP (Linux), defina uma nova senha para udpuser, conforme indicado a seguir:

   ```
   #sudo /opt/Arcserve/d2dserver/bin/d2duser --action=passwd --username=udpuser
   ```

   Observação: o nome de usuário padrão da interface do usuário de gerenciamento do Agente do Arcserve UDP (Linux) é udpuser.

9. (Opcional) Se quiser mudar para outro idioma, você pode modificar o arquivo de configuração no servidor do Agente do Arcserve UDP (Linux):

   /opt/Arcserve/d2dserver/nls/nls.cfg

   Em seguida, defina D2D_LANG=$OTHER_LANGUAGE e reinicie o d2dserver com o comando a seguir:

   #/opt/Arcserve/d2dserver/bin/d2dserver restart

   Observação: o inglês é o idioma padrão do Agente do Arcserve UDP (Linux).

   Agora, o Agente do Arcserve UDP (Linux) está pronto para uso na nuvem da AWS, e o URL para procurar o servidor de backup Linux é https://$INSTANCE_IP:8014.

   O Agente do Arcserve UDP (Linux) foi instalado com êxito na nuvem da AWS.

Verificar a instalação

Verifique se a instalação foi concluída depois de instalar o Agente do Arcserve UDP (Linux).

Siga estas etapas:

1. Abra um navegador em qualquer computador com Windows.
2. Digite o URL do servidor de backup Linux que é exibido na tela de instalação.

   Exemplo: https://nomehost:8014

   A página de logon do Agente do Arcserve UDP (Linux) é exibida.
3. Digite suas credenciais de logon raiz e clique em Logon.

   A interface de usuário do Agente do Arcserve UDP (Linux) é aberta.

   O Agente do Arcserve UDP (Linux) é instalado com êxito e verificado.

Como desinstalar o Agente do Arcserve UDP (Linux)

Desinstale o Agente do Arcserve UDP (Linux) pelo servidor de backup Linux para interromper a proteção de todos os seus nós.

O fluxograma a seguir mostra o processo de desinstalação do Agente do Arcserve UDP (Linux):

Execute estas tarefas para desinstalar o Agente do Arcserve UDP (Linux):

- Revisar as considerações sobre desinstalação
- Desinstalar o Agente do Arcserve UDP (Linux)
- Verificar a desinstalação

Revisar as considerações sobre desinstalação

Considere os seguintes pontos antes de iniciar a desinstalação:

- Você possui credenciais de logon raiz para o servidor de backup.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Desinstalar o Agente do Arcserve UDP (Linux)

É possível desinstalar o Agente do Arcserve UDP (Linux) usando a linha de comando do servidor de backup. O processo de desinstalação remove todos os arquivos e diretórios que são criados durante a instalação do software.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá para a pasta *bin* onde o Arcserve UDP para Linux está instalado com o seguinte comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin/
   ```

3. Execute o seguinte comando para desinstalar o Agente do Arcserve UDP (Linux):

   ```
   # ./d2duninstall
   ```

   Uma mensagem será exibida após a conclusão da desinstalação.

   O Agente do Arcserve UDP (Linux) é desinstalado do servidor.

Verificar a desinstalação

Verifique se o Agente do Arcserve UDP (Linux) foi removido do servidor após a conclusão do processo de desinstalação.

Vá para a seguinte pasta e verifique se o Agente do Arcserve UDP (Linux) foi removido:

```
/opt/Arcserve/d2dserver
```

Você verificou a desinstalação do Agente do Arcserve UDP (Linux). O Agente do Arcserve UDP (Linux) foi removido do servidor Linux.

Como atualizar o Agente do Arcserve UDP (Linux)

Atualize o Agente do Arcserve UDP (Linux) para a próxima release a fim de disponibilizar várias modificações e diversos aprimoramentos nos recursos e no desempenho do Agente do Arcserve UDP (Linux).

O diagrama a seguir exibe o processo de atualização do Agente do Arcserve UDP (Linux):

Execute estas tarefas para atualizar o Agente do Arcserve UDP (Linux):

- Considerações sobre a atualização
- Atualizar o Agente do Arcserve UDP (Linux)
- Verificar a atualização

Considerações sobre a atualização

Considere os seguintes pontos antes de iniciar a atualização:

- Certifique-se de programar a atualização quando as tarefas de backup não estiverem em execução.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Atualizar o Agente do Arcserve UDP (Linux)

Atualize o Agente do Arcserve UDP (Linux) para a próxima release a fim de disponibilizar várias modificações e diversos aprimoramentos nos recursos e no desempenho do Agente do Arcserve UDP (Linux).

Quando você instala a atualização, o Agente do Arcserve UDP (Linux) tenta detectar uma instalação existente.

- Se o Agente do Arcserve UDP (Linux) detecta uma instalação existente, ele executa automaticamente o processo de atualização. Todas as configurações existentes (por exemplo, arquivos de configuração e banco de dados) são salvas e atualizadas.
- Se o Agente do Arcserve UDP (Linux) não detecta nenhuma instalação existente, ele executa automaticamente uma nova instalação.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Faça download do pacote de instalação do Agente do Arcserve UDP (Linux) (arquivo *.bin) na pasta raiz.

   Importante: quando você faz download do arquivo do pacote de instalação em uma pasta local, o caminho completo dessa pasta local não pode conter nenhum caractere especial, exceto espaços em branco, e só deve incluir os seguintes caracteres: a-z, A-Z, 0-9, - e _.
3. Forneça a permissão de execução para o pacote de instalação.
4. Execute o seguinte comando para iniciar a instalação:

   ```
   ./<llinux_installation_file_name>.bin
   ```

   O pacote de instalação verifica a plataforma suportada e exibe uma mensagem de confirmação.

   Se uma plataforma sem suporte for detectada, digite Y e pressione Enter para confirmar a instalação da plataforma sem suporte.

   O pacote de instalação detecta uma instalação existente e exibe uma mensagem de confirmação para atualização.
5. (Opcional) Digite Y e pressione Enter para confirmar as dependências do aplicativo.

6. Digite Y e pressione Enter para confirmar a instalação.

   O pacote de instalação exibe as informações do contrato de licença.

7. Digite Y e pressione Enter para aceitar o contrato de licença.

   O processo de instalação do Agente do Arcserve UDP (Linux) é iniciado.

   Quando a instalação do pacote de utilitário de restauração estiver concluída, as informações de criação do Live CD são exibidas.

   O Live CD é criado no seguinte local:

   `/opt/Arcserve/d2dserver/packages`

   Observação: o Live CD é necessário para se obter o endereço IP do nó de destino ao executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal).

O Agente do Arcserve UDP (Linux) é atualizado com êxito.

Verificar a atualização

Verifique se a atualização foi concluída após a atualização do Agente do Arcserve UDP (Linux) para a próxima release. O servidor de backup armazena um backup dos arquivos de configurações existentes. Quando a verificação for concluída, exclua o backup dos arquivos de configurações existentes.

Siga estas etapas:

1. Abra um navegador em qualquer computador com Windows.
2. Insira o URL do servidor de backup.

   Exemplo: https://nomehost:8014

   A página de logon do Agente do Arcserve UDP (Linux) é exibida.
3. Digite suas credenciais de logon raiz e clique em Logon.

   A interface de usuário do Agente do Arcserve UDP (Linux) é aberta.
4. Verifique se o servidor e backup está funcionando corretamente.
5. Efetue logon no servidor de backup como usuário raiz.
6. Navegue até à pasta d2dserver.bak e exclua a pasta.

   `/opt/Arcserve/d2dserver.bak`

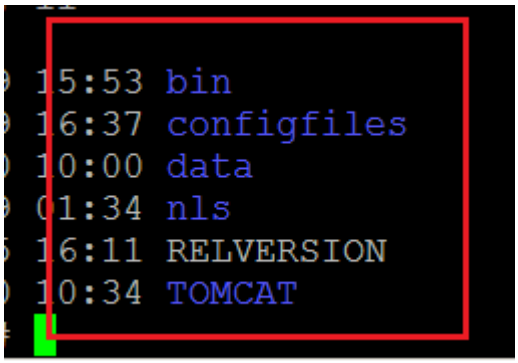
   O Agente do Arcserve UDP (Linux) é atualizado com êxito e verificado.

Como migrar o servidor de backup Linux de 32 bits para um servidor de 64 bits

A partir da versão 6, o Agente do Arcserve UDP (Linux) não aceitará nenhum servidor de 32 bits como o servidor de backup Linux. Para usar a versão 6 do Agente do Arcserve UDP (Linux), migre o servidor Linux de 32 bits para um servidor Linux de 64 bits.

Siga estas etapas:

1. Reserve os arquivos e as pastas a seguir na pasta de instalação do Agente do Arcserve UDP (Linux):



   Uma pasta de instalação típica para a versão 5 do Agente do Arcserve UDP (Linux) era '/opt/CA/d2dserver'/

   Observação: se a pasta do TOMCAT for uma pasta grande, reserve somente a pasta TOMCAT/conf.

2. Copie as pastas e arquivos reservados para algum outro local, como '/opt/d2dserver_32bit/'.
3. Compacte os arquivos e pastas reservados no seguinte local:

   ```
   tar -czf UDP_LINUX_AGENT.tar.gz /ultraconservative
   ```

4. Copie o arquivo compactado do sistema operacional Linux de 32 bits para o sistema operacional Linux de 64 bits usando SCP ou FTP.
5. Crie uma pasta no servidor do sistema operacional de 64 bits usando o seguinte comando:

   ```
   mkdir -p /opt/CA/d2dserver
   ```

6. Extraia o arquivo compactado no sistema operacional Linux de 64 bits usando o seguinte comando:

```
tar -xzf UDP_LINUX_AGENT.tar.gz
```

7. Copie os arquivos e pastas reservados no seguinte local:

   ```
   /opt/CA/d2dserver
   ```

   Por exemplo: cp -Rp /opt/d2dserver_32bit/* /opt/CA/d2dserver

8. Execute o pacote de instalação da versão 6.0 do Agente do Arcserve UDP (Linux) no servidor Linux de 64 bits.
9. O servidor de backup Linux atualiza automaticamente.

   Observação:: se o nome do host ou endereço IP for alterado, consulte Definir as configurações do sistema quando o nome do host ou endereço IP é alterado.

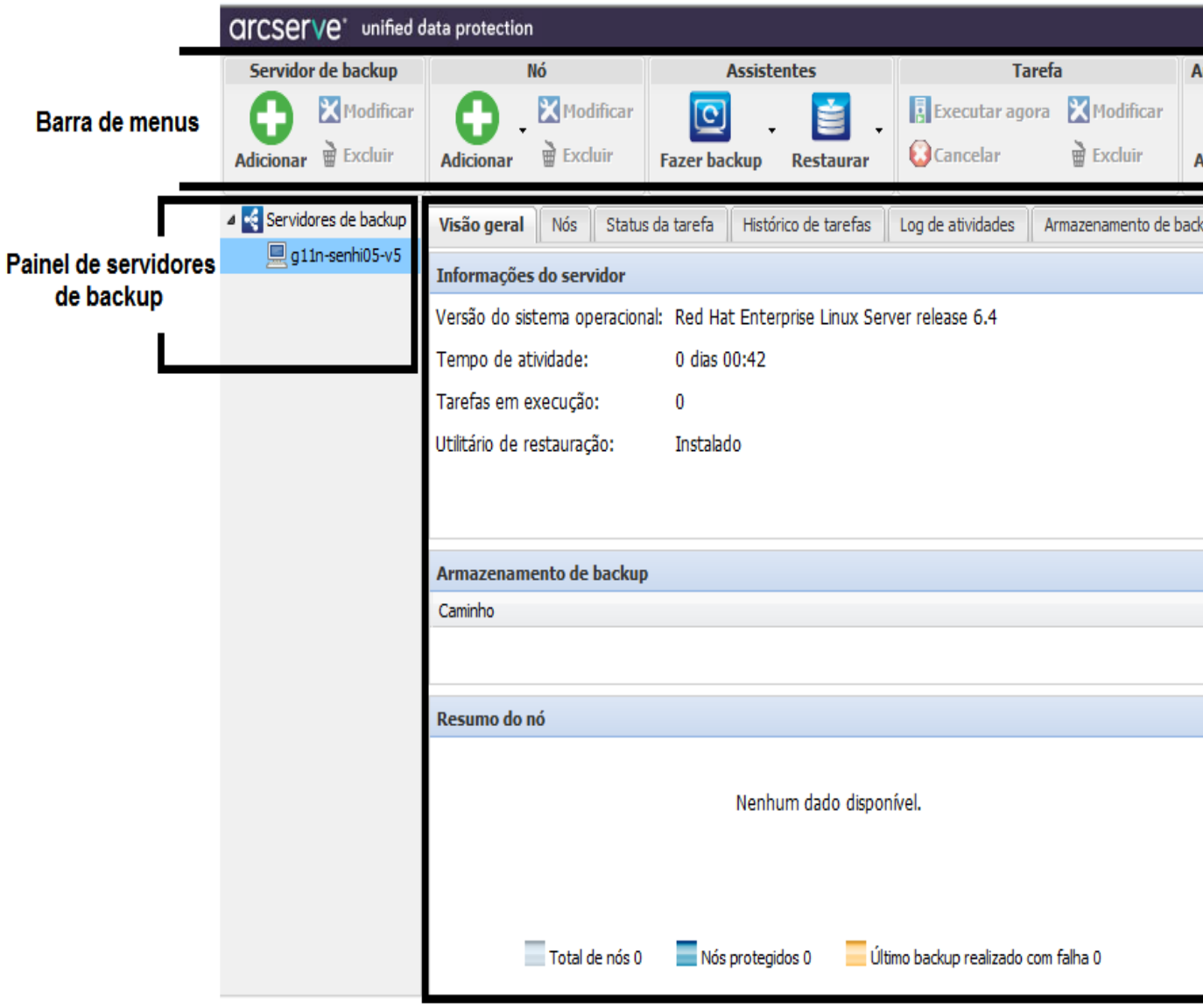
Capítulo 3: Interface do usuário

Esta seção contém os seguintes tópicos:

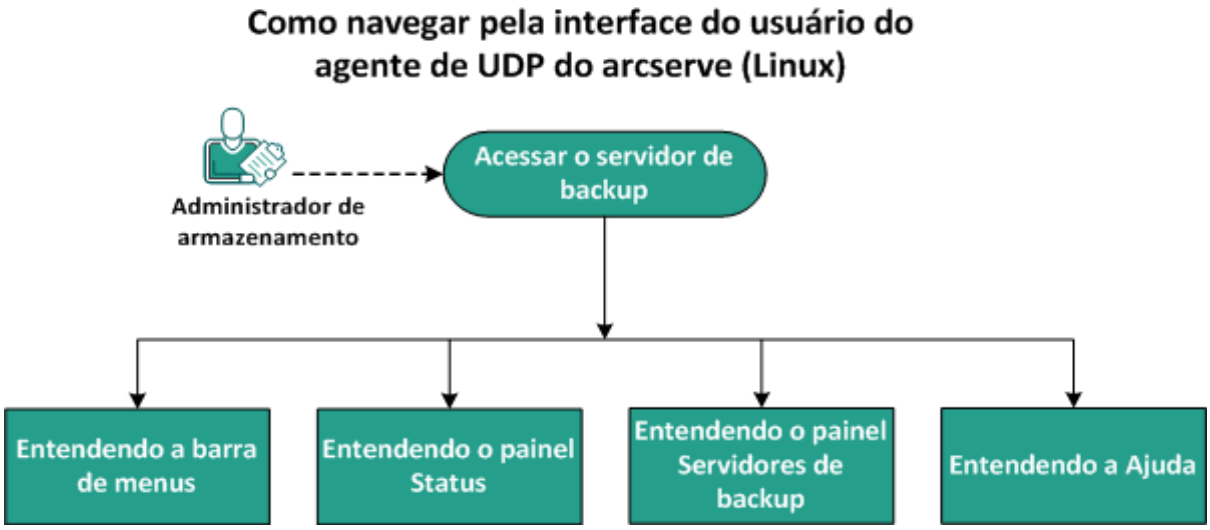
Como navegar pela interface do Agente do Arcserve UDP (Linux)

Antes de começar a usar o Agente do Arcserve UDP (Linux), você precisa se familiarizar com a interface do usuário. Na interface, é possível gerenciar os nós, gerenciar locais de armazenamento de backup, gerenciar as tarefas de backup e restauração e acessar os tópicos da ajuda.

A interface da página inicial inclui quatro áreas principais: barra de menus, painel Status, painel Servidores de backup e Ajuda.



O diagrama a seguir exibe o processo de navegação pela interface do Agente do Arcserve UDP (Linux):



Realize estas tarefas para iniciar a interface do servidor de backup:

- Acessar o servidor de backup
- Entendendo a barra de menus
- Entendendo o painel Status
- Entendendo o painel Servidores de backup
- Entendendo a Ajuda

Acessar o servidor de backup

Como gerenciador de armazenamento, é possível acessar o servidor de backup usando a interface web. Efetue logon com credenciais raiz ou não para acessar o servidor de backup. Use o endereço IP recebido durante a instalação do Agente do Arcserve UDP (Linux) para efetuar logon no servidor. Se você gravou o nome do host do servidor, pode efetuar logon no servidor por meio deste nome do host.

Observação: para obter mais informações sobre como fornecer a permissão de logon para os usuários não raiz, consulte Conceder permissões de logon a usuários não raiz.

Siga estas etapas:

1. Abra um navegador e digite o endereço IP do servidor de backup.

   Observação: por padrão, o servidor de backup segue o protocolo https e usa a porta 8014.

2. Digite as credenciais de logon e clique em Logon.

   A interface do servidor de backup é exibida.

   O servidor de backup é acessado com êxito.

Entendendo a barra de menus

A barra de menus permite realizar as seguintes tarefas:

- Gerenciar servidores de backup
- Gerenciar nós
- Gerenciar tarefas de backup
- Gerenciar tarefas de restauração
- Gerenciar locais de armazenamento de backup
- Filtrar pesquisas
- Atualizar páginas

A tela a seguir exibe a barra de menus:

A barra de menus inclui as seguintes opções:

Servidor de backup

Permite adicionar, modificar e excluir servidores que têm o Agente do Arcserve UDP (Linux) instalado. É possível instalar o Agente do Arcserve UDP (Linux) em vários servidores e gerenciar todos os servidores instalados a partir de uma IU central. Os nós que são gerenciados pelo servidor selecionado são exibidos no painel Status. Todos os servidores adicionados são exibidos no painel Servidores de backup. Não é possível modificar ou excluir o servidor central. Um servidor central é o primeiro servidor exibido no painel Servidores de backup. É possível modificar e excluir outros servidores pelo painel Servidores de backup. O botão Modificar permite atualizar apenas o número da porta dos servidores.

Nó

Permite adicionar, modificar e excluir nós dos quais deseja fazer backup. Nós são os computadores do quais você deseja fazer backup. É possível adicionar vários nós para fazer backup. Também é possível detectar nós que estão presentes na sua rede usando um script. É possível adicionar, no máximo, 200 nós para cada servidor.

Se excluir um nó, o servidor de backup limpará todas as informações sobre o nó do banco de dados, inclusive as informações de tarefas de backup. O servidor de backup também exclui os drivers do nó. Pode levar algum tempo para excluir os drivers completamente.

Assistentes

Permite iniciar o Assistente de backup e o Assistente de restauração para ajudar a guiá-lo durante o processo de backup e restauração.

- O Assistente de backup contém uma lista suspensa com três opções disponíveis:

  Fazer backup

  Use essa opção se você não tiver adicionado anteriormente nenhum nó a incluir no backup. A seleção desta opção abre o Assistente de backup e permite adicionar os nós durante o processo.

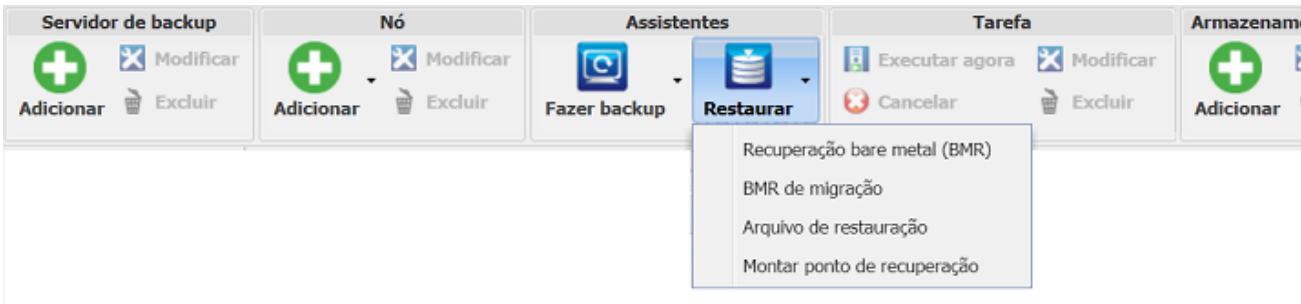
  Fazer backup dos nós selecionados

  Use essa opção se você já adicionou a nós anteriormente, antes de ativar o Assistente de backup. Se você clicar em Fazer backup dos nós selecionados sem adicionar nós nem selecionar os nós existentes, receberá uma mensagem de erro. Para evitar esse erro, selecione o nó na guia Nós e, em seguida, selecione Fazer backup dos nós selecionados.

  Adicionar os nós selecionados em uma tarefa existente

  Use essa opção se você já tiver uma tarefa de backup e desejar aplicar as mesmas configurações de backup para novos nós. Não é necessário configurar o Assistente de backup.

- O Assistente de restauração contém uma lista suspensa com três opções disponíveis:



BMR (Bare Metal Recovery - Recuperação Bare Metal)

Use essa opção para executar a BMR. É possível executar uma BMR usando o endereço IP ou o endereço MAC do computador bare metal a ser recuperado.

BMR de migração

Use essa opção para executar uma BMR de migração.

Restaurar arquivo

Use essa opção para executar uma restauração em nível de arquivo. É possível selecionar arquivos específicos a partir de um ponto de recuperação e restaurar esses arquivos.

Montar ponto de recuperação

Use essa opção para executar o recurso Montar ponto de recuperação. O MRP pode compartilhar arquivos em um ponto de recuperação por meio de NFS ou WebDAV. Para acessar esses arquivos, monte o local no servidor Linux.

Tarefa

Permite gerenciar as tarefas que você cria. Uma tarefa é uma instância de uma operação de backup ou restauração. Depois de criar uma tarefa de backup para um nó, não será necessário criar outra tarefa para executar um backup para o mesmo nó na próxima vez. No entanto, será necessário criar uma tarefa de restauração sempre que desejar executar uma BMR.

Armazenamento de backup

Permite adicionar e gerenciar os locais de armazenamento de backup. O local de armazenamento de backup pode ser o compartilhamento de NFS (Network File System – Sistema de Arquivos de Rede), o compartilhamento CIFS (Common Internet File System – Sistema de Arquivos de Internet Comum), Local ou o servidor RPS. Local é um caminho local no servidor de backup. O servidor RPS é um servidor de ponto de recuperação. O RPS é instalado quando você instala o Arcserve UDP. No RPS, é possível criar repositórios de dados nos quais você armazena os pontos de recuperação. Quando você adiciona um servidor RPS, também é necessário especificar o repositório de dados.

Quando você adiciona um local de armazenamento de backup, deve fornecer as credenciais para o local de armazenamento de backup selecionado. Só é possível modificar o nome de usuário e a senha do compartilhamento CIFS. Não é possível modificar os detalhes do compartilhamento NFS. Marque a

caixa de seleção Executar o script quando o espaço livre for menor que, para executar o script *backup_storage_alert.sh* quando o espaço livre for menor que o valor especificado. Esse valor pode ser uma porcentagem do espaço total no destino do backup ou uma quantidade mínima de espaço em disco (em MB) no destino do backup. O script backup_storage_alert.sh pode ser configurado para enviar um alerta quando o espaço livre disponível for menor do que o valor especificado.

Observação: para obter mais informações sobre como configurar o script backup_storage_alert.sh, consulte *Como integrar e automatizar o Agente do Arcserve UDP (Linux) com o ambiente de TI existente*.

Depois de adicionar um local de armazenamento de backup, é possível visualizar o tamanho total do arquivo correspondente e o espaço vazio no painel Status. Selecione um local de armazenamento de backup para ver os conjuntos de recuperação, os pontos de recuperação e a quantidade de espaço usada para cada nó que são copiados para backup no local de armazenamento de backup. Os destinos de armazenamento incluídos também são exibidos na página Destino do backup do Assistente de backup e na página Pontos de recuperação do Assistente de restauração.

Ferramentas

O menu de ferramentas inclui o botão Atualizar e o botão Filtro.

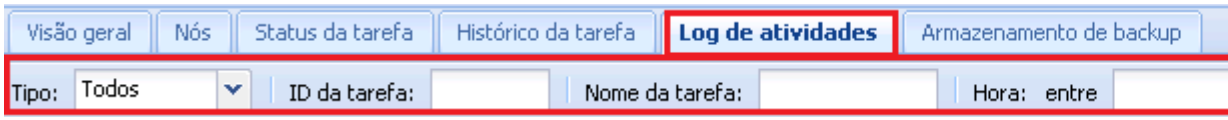
Atualizar

Permite atualizar a área de exibição selecionada no painel Status, incluindo o Log de atividades, para exibir as mensagens de status de restauração ou de backup mais recentes.

Filter

Permite filtrar as informações exibidas no painel Status com base nas informações fornecidas. O botão Filtro atua como um comutador para poder mostrar e ocultar os filtros usando o mesmo botão. Quando você escolhe mostrar os filtros, os campos de pesquisa são exibidos no painel Status. Quando você oculta os filtros, os campos de pesquisa são removidos do painel Status.

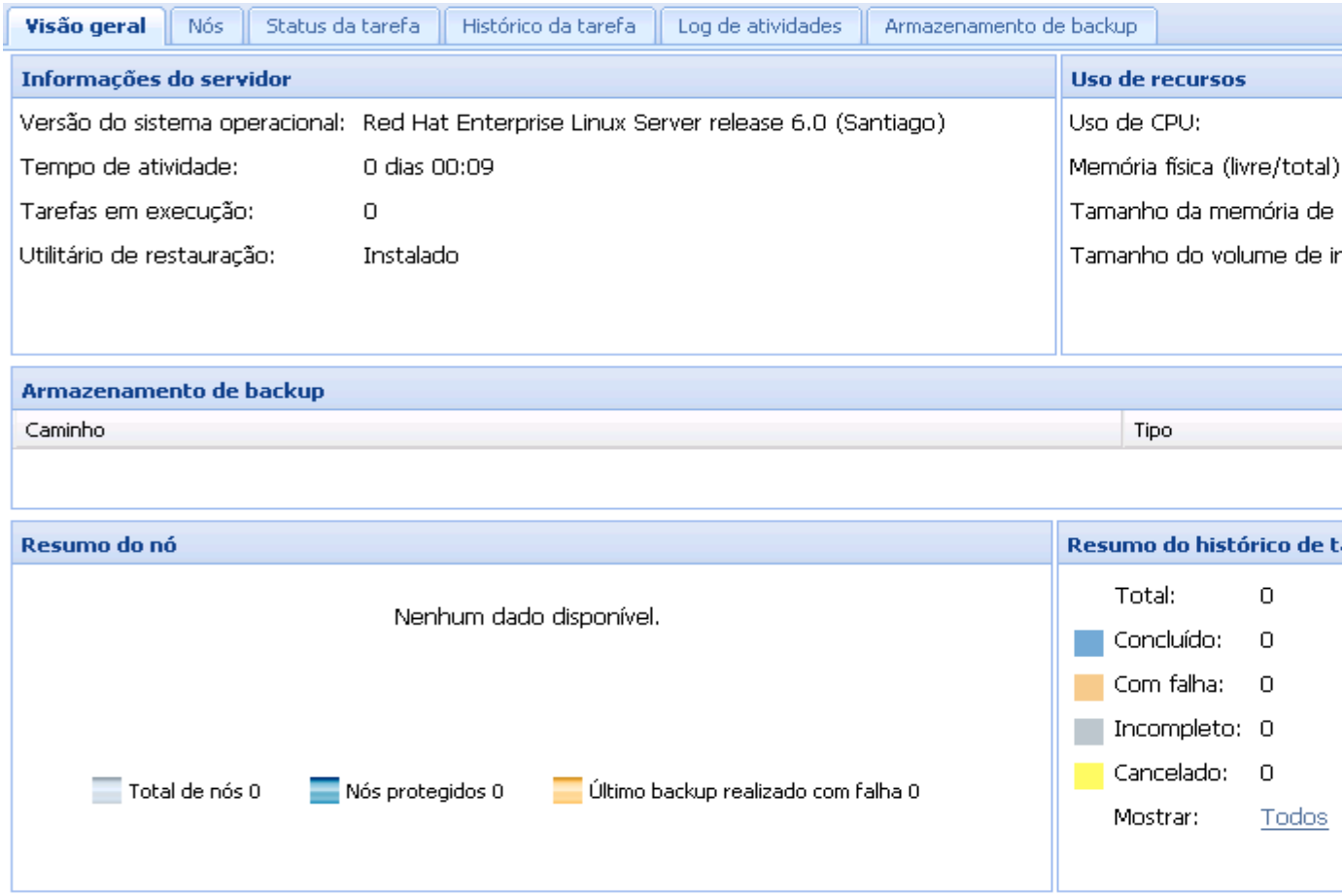
A tela a seguir exibe os filtros aplicados ao Log de atividades:



Entendendo o painel Status

O painel Status é a área que exibe todas as informações na interface do usuário. O painel Status inclui seis guias que permitem exibir informações com base na guia selecionada.

A tela a seguir exibe o painel Status:



O painel Status inclui as seguintes guias:

Visão geral

Fornece um resumo dos seguintes itens:

Informações do servidor

Exibe a versão do sistema operacional, o tempo decorrido desde a inicialização do servidor e as informações de licenciamento do Agente do Arcserve UDP (Linux). Também exibe se o utilitário de restauração está instalado neste servidor.

Uso de recursos

Exibe o uso da CPU, o tamanho da memória física e de troca, total e disponível. Exibe também o tamanho do volume de instalação.

Armazenamento de backup

Exibe todos os locais de sessões de backup que foram adicionados e o espaço disponível em cada local. Essas informações ajudam a planejar o próximo local de backup, dependendo do espaço de armazenamento disponível.

Resumo de nós

Exibe uma representação gráfica dos nós protegidos e nós com as últimas tentativas de backup sem êxito. Resumo de nós inclui as seguintes categorias:

Total de nós exibe o número de nós incluídos no Agente do Arcserve UDP (Linux), independentemente do status de backup.

Nós protegidos exibe o número de nós cujo último backup foi bem-sucedido que são considerados como protegidos caso seja necessária uma recuperação.

Último backup realizado com falha exibe o número de nós cujo backup mais recente não foi bem-sucedido (com falha, cancelado, incompleto). Dependendo da causa da falha do backup, alguns desses nós ficarão desprotegidos no caso de uma recuperação ser necessária.

Resumo do histórico de tarefas

Exibe um gráfico de pizza que resume o histórico de todas as tarefas. O resumo não inclui as tarefas em execução.

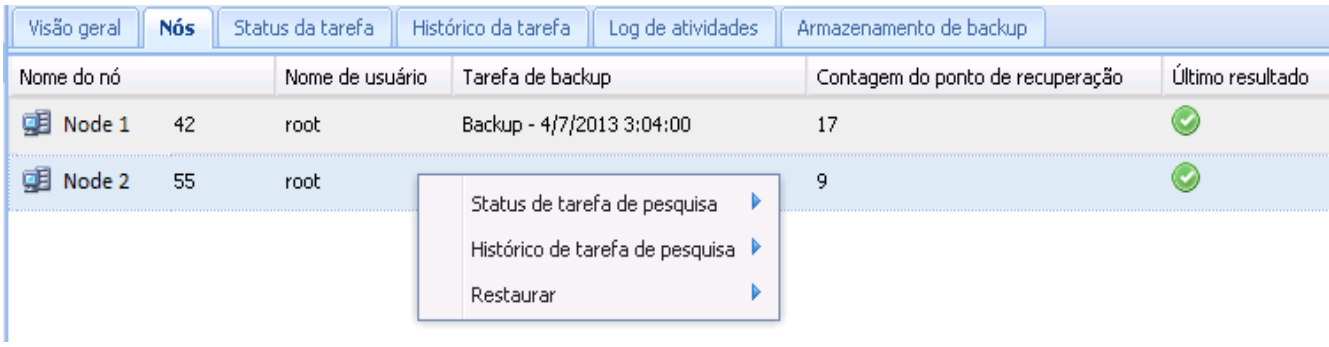
Os seguintes campos não são autoexplicativos:

- Incompleto exibe o número de tarefas que foram executadas com êxito com alterações mínimas. Por exemplo, ao fazer a restauração de arquivos do Red Hat 6 para o Red Hat 5, os arquivos são restaurados com êxito, mas alguns atributos estão ausentes nos arquivos restaurados.
- Outros exibe o número de tarefas que você cancelou.

Nós

Exibe todos os nós adicionados ao servidor de backup. É possível aplicar filtros à guia Nós para pesquisar os nós necessários. A guia Nós também inclui um menu de contexto. O menu de contexto permite que você pesquise o status da tarefa ou o histórico de tarefas do nó selecionado. O menu de contexto também permite restaurar os dados. É possível filtrar o histórico de tarefas ou o status da tarefa usando o nome da tarefa ou o nome do nó. Se você pesquisar o

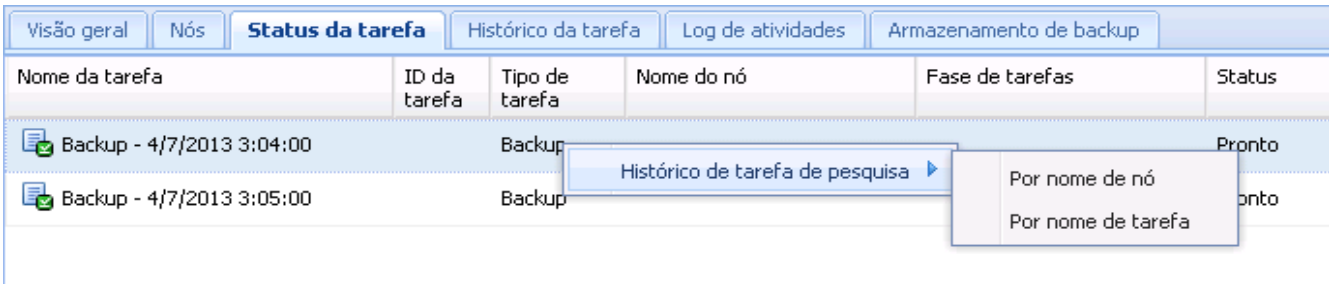
histórico da tarefa do nó selecionado, a guia Histórico da tarefa será aberta com o filtro de pesquisa aplicado à guia. Da mesma forma, se você pesquisar o status da tarefa, a guia Status da tarefa será aberta com o filtro de pesquisa aplicado à guia. A opção Restaurar permite executar a BMR ou a restauração no nível de arquivo. Ele abre o Assistente de restauração e exibe todos os pontos de recuperação do nó selecionado.



Status da tarefa

Exibe a lista de tarefas de backup e restauração criadas, incluindo o status de cada tarefa. Use essa guia para executar uma tarefa de backup ou de restauração e execute novamente a tarefa de backup. É possível ver o andamento das tarefas de backup ou restauração executadas. É possível aplicar filtros à guia Status da tarefa para pesquisar os nós necessários. A guia Status da tarefa também inclui um menu de contexto. O menu de contexto permite que você pesquise o histórico de tarefas referente à tarefa selecionada. É possível filtrar o histórico de tarefas usando o nome da tarefa ou o nome do nó. Se você pesquisar o histórico de tarefas da tarefa selecionada, a guia Histórico da tarefa será aberta com o filtro de pesquisa aplicado à guia.

A tela a seguir exibe o menu de contexto da guia Status da tarefa:



Histórico de tarefas

Exibe a lista de tarefas de backup e restauração que foram previamente executadas. É possível aplicar filtros à guia Histórico da tarefa para pesquisar o histórico de tarefa necessário. Ao selecionar uma tarefa, o status da tarefa é exibido na parte inferior da página.

Log de atividades

Exibe uma lista de mensagens de processamento e mensagens de status das tarefas de backup e de restauração. Atualize o Log de atividades para obter as últimas mensagens de tarefas de backup e restauração recentes. É possível aplicar filtros à guia Log de atividades para pesquisar os logs de atividades necessários.

Armazenamento de backup

Exibe o destino do backup que você adicionou na barra de menus. É possível ver o espaço livre de armazenamento e gerenciar o destino do backup. Essa opção é útil se você deseja saber o espaço livre disponível em determinado destino de backup para planejar seu backup. Quando você adiciona um destino de armazenamento, esse destino aparece no Assistente de backup.

Entendendo o painel Servidores de backup

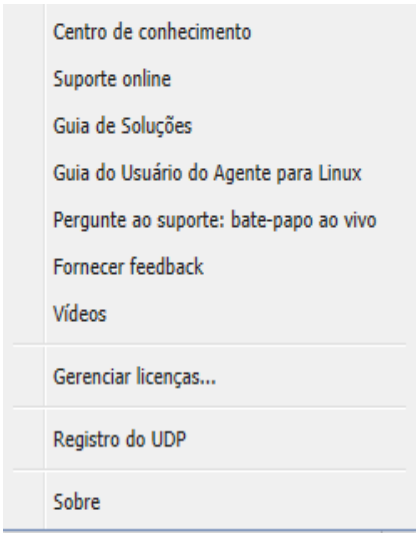
O painel Servidores de backup exibe a lista de servidores de backup gerenciados pelo servidor atual. É possível adicionar servidores na barra de menus e gerenciar todos os servidores a partir de uma interface. Se você tiver adicionado vários servidores, o painel Status exibe o status do servidor selecionado. Cada servidor pode gerenciar, no mínimo, 200 nós clientes.

Em geral, o primeiro servidor exibido no painel Servidores de backup é o principal servidor de backup, e os outros são integrantes. Para gerenciar vários servidores a partir de um servidor central, verifique se a versão do servidor central e dos servidores integrantes são iguais.

A tela a seguir exibe o painel Servidores de backup:

Entendendo a Ajuda

A caixa de diálogo Ajuda permite acessar os tópicos de Ajuda do Agente do Arcserve UDP (Linux). É possível executar as seguintes tarefas na lista suspensa Ajuda:



As opções a seguir estão disponíveis na lista suspensa Ajuda:

Centro de conhecimento

Permite acessar a biblioteca.

Suporte online

Permite acessar o site de suporte da Arcserve.

Guia de Soluções

Permite acessar a versão HTML do Guia de soluções do agente do Arcserve UDP.

Guia do Usuário do Agente para Linux

Permite acessar a versão HTML do Guia do usuário.

Pergunte ao suporte: bate-papo ao vivo

Permite abrir uma janela de bate-papo e entrar em contato com um executivo do suporte da Arcserve para uma conversa ao vivo.

Fazer comentários

Permite acessar o site de suporte da Arcserve e fornecer comentários para a equipe de desenvolvimento.

Vídeos

Permite acessar os vídeos e tutoriais online relacionados ao Agente do Arcserve UDP (Linux).

Gerenciar licenças

Permite acessar a caixa de diálogo Gerenciamento de licenças e gerenciar todas as licenças de uma interface central.

Programa de melhoria do produto

Permite fornecer sugestões para aprimorar o produto da Arcserve.

Sobre

Permite visualizar as informações do produto (número da versão e número de compilação) e acessar as Notas da Versão do agente do Arcserve UDP.

Registrar o Arcserve UDP

Depois de instalar o Arcserve UDP, é necessário registrar o produto a partir do console. Esse registro permite que a Arcserve colete automaticamente as estatísticas e os dados de uso do console.

Importante: a Arcserve não coleta nenhuma informação crítica pessoal ou comercial, como nome do nó, endereço IP, credenciais de logon, nome de domínio e nomes de rede.

Se não tiver registrado o console, você receberá a seguinte notificação na guia **Mensagens** do console.

```
Sua cópia do Arcserve Unified Data Protection não foi registrada no Programa de Aprimoramento do Produto da Arcserve. Faça o registro.
```

Siga estas etapas:

1. No Console, clique em **Ajuda**, **Programa de Aprimoramento do Produto**.

   A caixa de diálogo **Programa de aprimoramento do produto da Arcserve** é aberta.

2. Selecione a caixa de seleção **Participar do programa de aprimoramento do produto da Arcserve**.
3. Especifique os seguintes detalhes:

   Nome

   Digite seu nome.

   Empresa

   Digite o nome de sua empresa.

   Telefone

   Digite seu número de telefone no seguinte formato:

   Código de país - Número de telefone. Por exemplo: 000-1122334455

   Endereço de email

   Digite seu endereço de email. Este é um campo obrigatório. O email de verificação será enviado para esse endereço de email.

   Fulfillment Number

   Especifique o Fulfillment Number. Você deve ter recebido esse número por email quando fez download do Arcserve UDP.

4. Clique em **Enviar o email de verificação**.

   O email de verificação é enviado para o endereço de email que você mencionou na caixa de diálogo **Programa de aprimoramento do produto da Arcserve**.

5. Efetue logon na conta de email e abra o email recebido.
6. Clique no link de verificação fornecido no email.

   Você registrou o Arcserve UDP com êxito.

   Após o registro, o botão Cancelar participação é ativado.

   Para cancelar o registro, clique em **Cancelar participação**.

   se você deseja atualizar o endereço de email, é necessário fazer o registro novamente. Para fazer o registro novamente, execute o mesmo processo conforme descrito neste tópico.

Capítulo 4: Usando o Agente do Arcserve UDP (Linux)

Esta seção contém os seguintes tópicos:

Como gerenciar as licenças

O Agente do Arcserve UDP (Linux) exige que você licencie seu produto para receber acesso autorizado e ininterrupto aos componentes relacionados. Além disso, se você quiser implantar o Arcserve UDP para Linux em locais remotos, será preciso licenciar esses locais remotos para aproveitar os benefícios que o Agente do Arcserve UDP (Linux) oferece.

O Agente do Arcserve UDP (Linux) funcionará por um período de 30 dias após o início do uso. Em seguida, aplique uma chave de licença apropriada para continuar a usá-lo. O Agente do Arcserve UDP (Linux) permite que você gerencie as licenças de todos os servidores de backup Linux em uma interface central.

O diagrama a seguir mostra o processo para gerenciar licenças:

Conclua as tarefas a seguir para gerenciar as licenças:

- Acessar o gerenciador de licenças
- Noções básicas sobre a caixa de diálogo Gerenciamento de licenças
- Gerenciar as licenças

Acessar o gerenciador de licenças

É preciso acessar a caixa de diálogo Gerenciamento de licenças pela interface da web do Agente do Arcserve UDP (Linux) para gerenciar todas as licenças.

Siga estas etapas:

1. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
2. Na página inicial, clique em Ajuda, Gerenciar licenças.

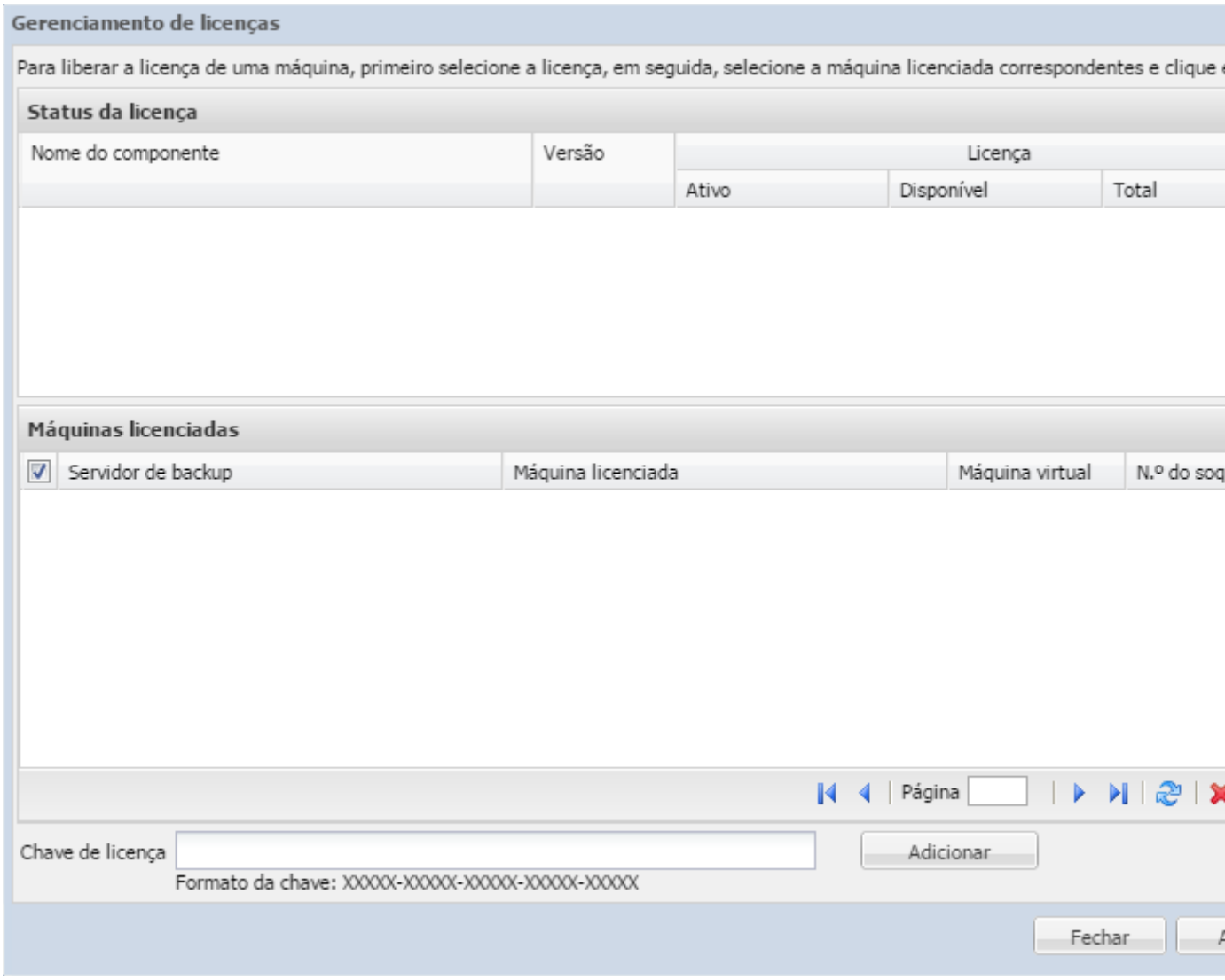
   A caixa de diálogo Gerenciamento de licenças será aberta.

   O gerenciador de licenças é acessado.

Noções básicas sobre a caixa de diálogo Gerenciamento de licenças

A caixa de diálogo Gerenciamento de licenças permite que você gerencie todas as licenças do Agente do Arcserve UDP (Linux). É possível gerenciar as licenças de vários servidores de backup a partir de uma única interface.

A tela a seguir exibe a caixa de diálogo Gerenciamento de licenças:



A caixa de diálogo Gerenciamento de licenças é dividida em duas seções: Status da licença e Máquinas licenciadas.

Status da licença

Nome do componente

Identifica o nome da licença.

Versão

Identifica o número da release da licença.

Ativo

Identifica o número de licenças que estão sendo usadas no momento para fazer backup dos nós.

Disponível

Identifica o número de licenças que ainda estão disponíveis no pool de licenças e pode ser usado para fazer backup de computadores Linux.

Total

Identifica o número total de licenças obtidas para fazer backup do computador. O total é a soma das licenças disponíveis e ativas.

Máquinas licenciadas

Servidor de backup

Identifica o servidor Linux onde você instalou o Agente do Arcserve UDP (Linux).

Máquinas licenciadas

Identifica os computadores Linux para os quais você aplicou uma licença a fim de protegê-los.

Gerenciar as licenças

É possível adicionar e liberar licenças a partir da caixa de diálogo Gerenciamento de licenças. A licença adicionada é exibida na caixa de diálogo Gerenciamento de licenças. Se não desejar mais fazer backup de um computador, você pode liberar a licença desse computador.

Para adicionar uma licença, siga estas etapas:

a. Usando o Portal de licenças do Arcserve, gere a chave de licença. Para obter detalhes, consulte Como gerar chaves de licença do Arcserve para agentes autônomos.

b. Insira a chave de licença no campo Chave de licença da caixa de diálogo Gerenciamento de licenças e clique em Adicionar.

c. Feche e abra a caixa de diálogo Gerenciamento de licenças.

A licença é adicionada e é listada na área Status da licença.

Para liberar uma licença, siga estas etapas:

a. Selecione a licença na área Status da licença da caixa de diálogo Gerenciamento de licenças.

b. Selecione o servidor de backup em Máquinas licenciadas e clique em Liberar.

c. Feche e abra a caixa de diálogo Gerenciamento de licenças.

A licença é liberada do computador.

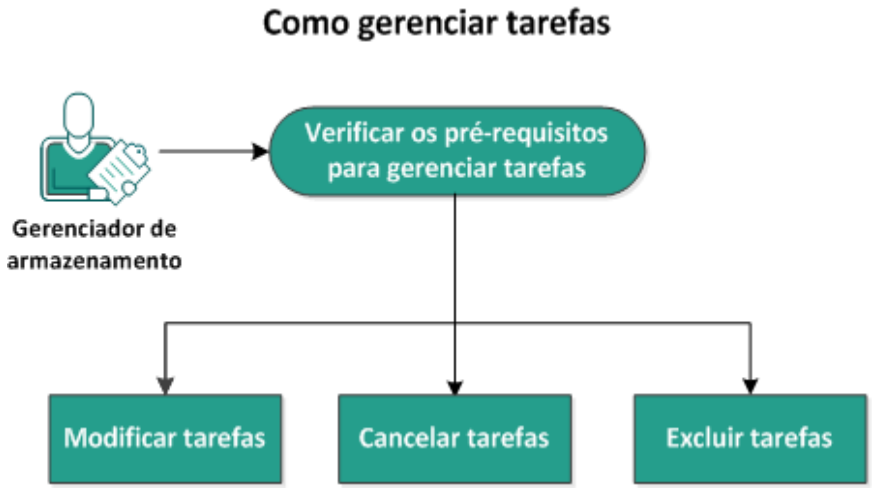
As licenças são gerenciadas com êxito.

Como gerenciar tarefas

Depois de criar uma tarefa de backup ou de restauração, é possível gerenciar todas as tarefas no menu Tarefas. Gerenciar uma tarefa inclui as seguintes tarefas:

- Modificação de tarefas
- Cancelamento de uma tarefa
- Exclusão de tarefas

O diagrama a seguir exibe o processo para gerenciar tarefas:



Realize essas tarefas para gerenciar suas tarefas:

- Verificar os pré-requisitos
- Modificar tarefas
- Cancelar tarefas
- Excluir tarefas

Verificar os pré-requisitos para gerenciar tarefas

Considere os pré-requisitos a seguir antes de gerenciar suas tarefas:

- Você tem uma tarefa válida para gerenciar
- Você tem a permissão apropriada para gerenciar tarefas.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Modificar tarefas

É possível abrir qualquer tarefa existente e modificar as configurações da tarefa a partir da interface da web. Por exemplo, se você deseja alterar o destino do backup para um computador que já está protegido, não será necessário criar uma nova tarefa. É possível abrir a tarefa existente que protege o computador e modificar somente a seção de destino do backup. Todas as outras configurações permanecem inalteradas, exceto as configurações de destino do backup.

Siga estas etapas:

1. Selecione uma tarefa a partir da guia Status da tarefa.
2. Clique em Modificar no menu Tarefa.

   O assistente para a tarefa selecionada é aberto.
3. Modifique as configurações no assistente.
4. Clique em Enviar na página Resumo do assistente.

   A tarefa é enviada e é executada de acordo com suas configurações.

   A tarefa é modificada com êxito.

Cancelar tarefas

É possível cancelar uma tarefa em execução pela interface da web do Agente do Arcserve UDP (Linux).

Siga estas etapas:

1. Selecione uma tarefa a partir da guia Status da tarefa.
2. Clique em Cancelar no menu Tarefa.

   A caixa de diálogo Cancelar a tarefa é aberta.

3. Selecione uma das opções a seguir na lista suspensa Cancelar a tarefa de:

   Nó selecionado

   Especifica que a tarefa é cancelada somente para o nó selecionado.

   Todos os nós protegidos pela tarefa selecionada

   Especifica que a tarefa é cancelada para todos os nós protegidos pela tarefa selecionada.

4. Clique em OK.

   A tarefa é cancelada.

Excluir tarefas

É possível excluir uma tarefa quando não se deseja mais proteger ou restaurar um computador. Também é possível excluir uma tarefa que protege um grupo de nós. Ao excluir uma tarefa, os pontos de recuperação cujo backup foi feito anteriormente ainda permanecem disponíveis no destino de backup especificado. É possível usar esses pontos de recuperação para restaurar os dados.

Para uma tarefa em execução, a opção Excluir é inativa. É necessário cancelar a tarefa em execução e, em seguida, excluir a tarefa.

Siga estas etapas:

1. Selecione uma tarefa a partir da guia Status da tarefa.
2. Clique em Excluir no menu Tarefa.

   A caixa de diálogo Excluir a tarefa é aberta.

3. Selecione uma das opções a seguir na lista suspensa Excluir a tarefa de:

   Nó selecionado

   Especifica que a tarefa é excluída somente para o nó selecionado.

   Todos os nós protegidos pela tarefa selecionada

   Especifica que a tarefa é excluída para todos os nós protegidos pela tarefa selecionada.

4. Clique em OK.

   A tarefa é excluída.

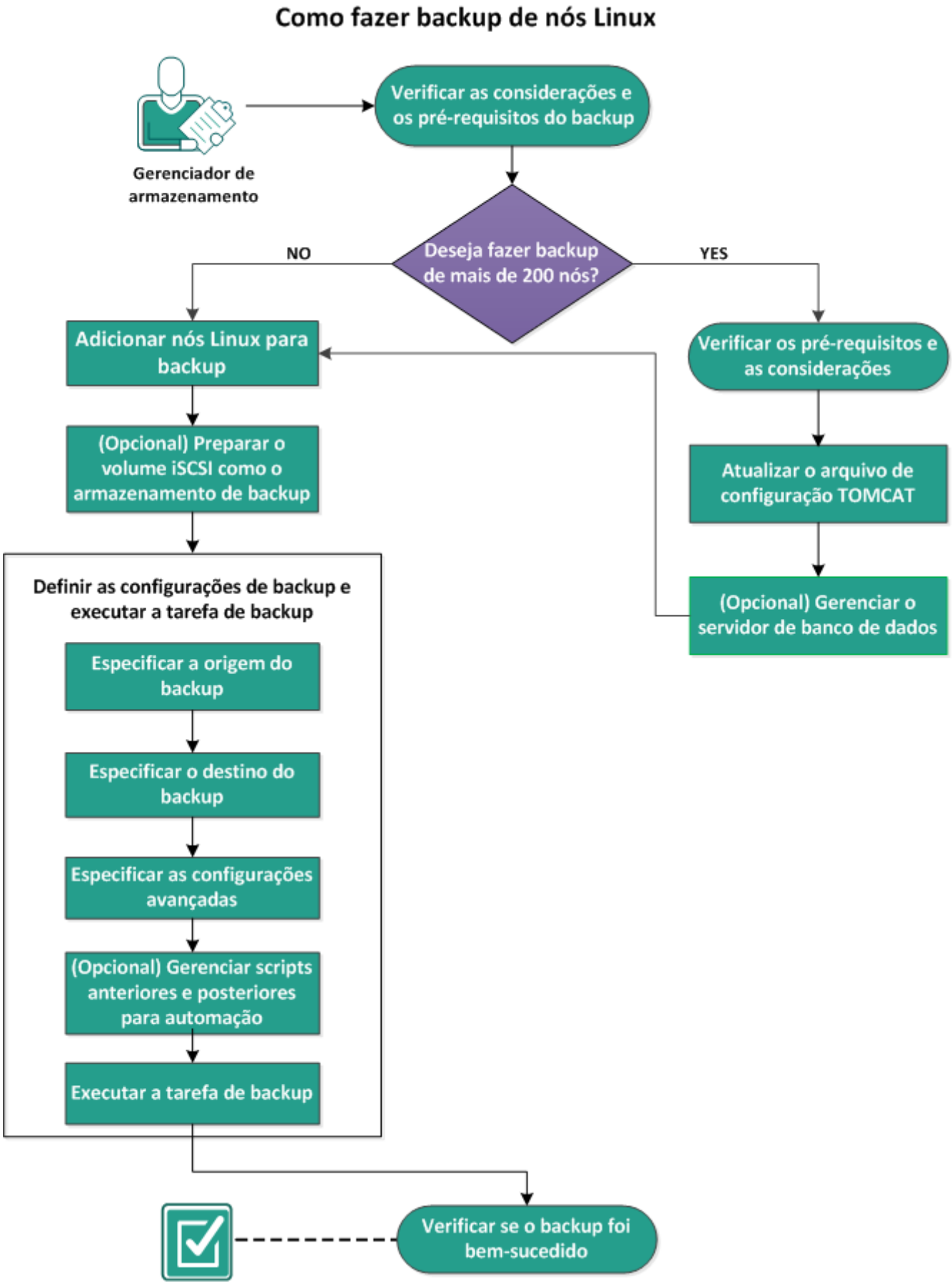
Como fazer backup de nós Linux

O Agente do Arcserve UDP (Linux) permite que você faça backup de nós do Linux e dos dados armazenados nele. Também é possível fazer backup do servidor de backup como qualquer outro nó Linux. O servidor de backup pode fazer backup de um máximo de 200 nós.

Quando o Agente do Arcserve UDP (Linux) faz backup dos dados, ele também captura informações relacionadas ao sistema operacional, aos aplicativos instalados e aos drivers (entre outras) do nó de produção. Como resultado, quando você restaura os dados de backup, é possível executar uma BMR ou restaurar arquivos específicos de sua necessidade.

Observação: se você reiniciar o nó de origem do backup, o próximo backup será convertido em um Backup de verificação (para backup sem redução de redundância) ou em um Backup completo (para backup de redução de redundância).

O diagrama a seguir exibe o processo para fazer backup de nós Linux:


Como fazer backup de nós Linux
Gerenciador de armazenamento
Verificar as considerações e os pré-requisitos do backup
Deseja fazer backup de mais de 200 nós?
NO
YES
Adicionar nós Linux para backup
(Opcional) Preparar o volume iSCSI como o armazenamento de backup
Definir as configurações de backup e executar a tarefa de backup
Especificar a origem do backup
Especificar o destino do backup
Especificar as configurações avançadas
(Opcional) Gerenciar scripts anteriores e posteriores para automação
Executar a tarefa de backup
Verificar os pré-requisitos e as considerações
Atualizar o arquivo de configuração TOMCAT
(Opcional) Gerenciar o servidor de banco de dados
Verificar se o backup foi bem-sucedido

Realize essas tarefas para fazer backup de um nó Linux:

- Verificar as considerações e os pré-requisitos do backup
- Deseja fazer backup de mais de 200 nós
  - Verificar os pré-requisitos e as considerações
  - Atualizar o arquivo de configuração TOMCAT
  - Gerenciar o servidor de banco de dados
- Adicionar nós Linux para backup
- (Opcional) Registrar a chave pública do Arcserve para inicialização segura
- (Opcional) Preparar o volume iSCSI como o armazenamento de backup
- Definir as configurações de backup e executar a tarefa de backup
  - Especifique a Origem do backup
  - Especifique o Destino do backup
  - Especificar as configurações avançadas
  - (Opcional) Gerenciar scripts anteriores e posteriores para automação
  - Executar a tarefa de backup
- Verificar se o backup foi bem-sucedido

Verificar as considerações e os pré-requisitos do backup

Verifique os seguintes requisitos antes de executar um backup:

- Você tem os requisitos de hardware e software suportados para o nó de backup.

  Observação: para obter mais informações sobre os requisitos de hardware e software suportados, consulte as *Notas da Versão do Arcserve UDP*.

- Você tem um destino válido para armazenar os dados de backup.
- Você possui os nomes de usuário e senhas de nós dos quais deseja fazer backup.
- A pasta */tmp* no nó de backup tem um mínimo de 300 MB de espaço. A pasta */tmp* é usada para processar o acúmulo de blocos incrementais.
- Os scripts perl e sshd (Daemon de SSH) são instalados nos nós de que deseja fazer backup.
- O nó de backup pode acessar o destino do backup e você tem permissão de gravação.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais suportados.

Para executar novamente uma tarefa de backup, verifique se você fez o backup do nó antes e se tem uma tarefa de backup válida.

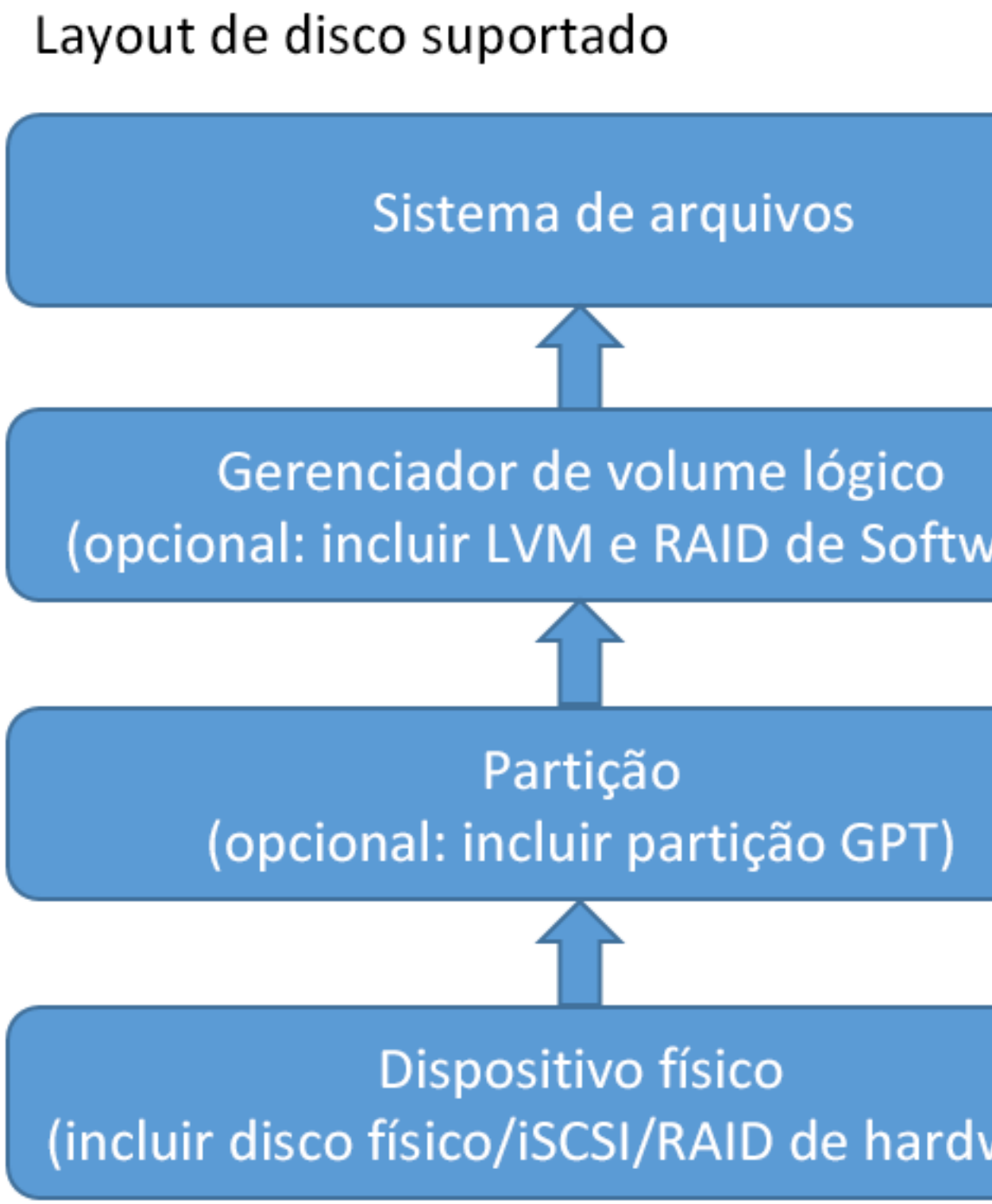
Verifique as seguintes considerações de backup:

- Para otimizar o gerenciamento dos pontos de recuperação, você deve considerar a seguinte recomendação ao agendar a frequência dos seus backups:
  - Para os sistemas protegidos com backups incrementais executados a cada 15 minutos, é recomendável agendar um backup completo a cada semana (para atualizar a imagem de base).

  Observação: se a quantidade de espaço usada para o armazenamento de imagens de backup for uma preocupação, você deve considerar a programação de backups completos com menos frequência para usar menos espaço de armazenamento.

Layout de disco suportado pelo Agente do Arcserve UDP (Linux)

A ilustração a seguir mostra o layout do disco que é suportado pela origem de backup do agente do Arcserve UDP (Linux):


Layout de disco suportado
Sistema de arquivos
Gerenciador de volume lógico
(opcional: incluir LVM e RAID de Softw
Partição
(opcional: incluir partição GPT)
Dispositivo físico
(incluir disco físico/iSCSI/RAID de hardv
* Não há suporte para LVM e RAID de software aninhados.

Disco suportado pelo Agente do Arcserve UDP (Linux)

Diferentes tipos de disco são suportados para os discos de backup e de origem de backup do Agente do Arcserve UDP (Linux). A matriz a seguir lista os tipos de disco que são suportados para cada função.

Suporte a backup e BMR		
Tipo de disco (volume)	**Como origem de backup**	**Como destino de backup**
Volume montado (Partição de disco tradicional e LVM ***2**)	Sim	Sim
Volume RAW (não formatado)	Não	Não
Volume criptografado	Não	Não
Trocar	Não	Não apli-cável
Disco de tabela de partição GUID:		
■ Disco de dados de tabela de partição GUID	Sim	Sim
■ Disco de inicialização de tabela de partição GUI	Sim	Não apli-cável
Disco RAID *1:		
■ Software RAID (RAID-0 (stripe))	Sim	Sim
■ Software RAID (RAID-1 (duplicado))	Sim	Sim
■ RAID-5 de software	Sim	Sim
■ Hardware RAID (incluir RAID integrado)	Sim	Sim
Sistema de arquivos:		
■ EXT2	Sim	Sim
■ EXT3	Sim	Sim
■ EXT4	Sim	Sim
■ Reiserfs Versão 3	Sim	Sim
■ XFS *3	Sim	Sim
■ Btrfs *4	Sim	Sim
Volume compartilhado:		
■ Volume compartilhado do Windows (Compartilhamento do CIFS)	Não apli-cável	Sim
■ Volume compartilhado do Linux (Samba compartilhado)	Não	Sim
■ Compartilhamento de NFS do Linux	Não	Sim

Tipo de dispositivo:		
■ Disco removível (ex.: cartão de memória, RDX)	Sim	Sim
*1	O RAID falso, também chamado de RAID incorporado, fornecido pelo BIOS na placa-mãe não é suportado pelo Agente do Arcserve UDP (Linux).	
*2	Não há suporte para LVM integrado.	
*3	A restauração em nível de arquivo para uma versão mais recente do XFS não tem suporte em um servidor de backup Linux que tenha uma versão anterior do XFS. Por exemplo, a restauração em nível de arquivo para o XFS no RHEL7.X não tem suporte no RHEL6.x funcionando como servidor de backup. No entanto, uma outra opção seria usar o Live CD como um servidor de backup temporário para executar a restauração em nível de arquivo. **Observação:** o Redhat Enterprise Linux 8, CentOS 8 e Oracle Linux 8 têm limitações que não podem suportar o sistema de arquivos BMR, IVM e AR for XFS na compilação		

	do Arcserve UDP 7.0 U1.
*4	Não há suporte para a restauração em nível de arquivo no computador de origem (por exemplo, instale o servidor de backup Linux no computador A, faça backup do computador A e execute a restauração a partir do ponto de recuperação A no computador A). Não há suporte a filtros de arquivo ou de pasta. O processo de equilíbrio/scrubbing de sistema de arquivo será cancelado no início do backup. Suporte a RAID do BTRFS: RAID-0 e RAID-1. Interface do usuário do filtro de volume: somente o volume principal é exibido. Isso não é uma limitação, mas um comportamento esperado.

Deseja fazer backup de mais de 200 nós

Um servidor de backup pode gerenciar um máximo de 200 nós por padrão. Se tiver mais de 200 nós para backup, será possível configurar Servidores de backup integrantes. Em seguida, use um servidor de backup central para gerenciar todos os seus servidores integrantes.

Se tiver um servidor de backup dedicado e mais de 200 nós a gerenciar, será possível ativar as configurações específicas e gerenciar mais de 200 nós.

Verificar os pré-requisitos e as considerações

Verifique os seguintes pré-requisitos antes de fazer backup de mais de 200 nós do Linux:

- Somente o Linux de 64 bits é suportado para o servidor de backup
- O servidor de backup deve ser um servidor dedicado. O Agente do Arcserve UDP (Linux) modifica as configurações do sistema para atender ao requisito de alta escalabilidade do servidor.
- O servidor deve atender aos seguintes requisitos mínimos de hardware. Se tiver um grande número de nós, as especificações de hardware devem ser maiores do que os requisitos mínimos.
  - Memória de 8 GB
  - Espaço em disco livre de 10 GB para a pasta /opt

Revise as seguintes considerações:

- Quando você ativa o Agente do Arcserve UDP (Linux) para fazer backup de mais de 200 nós, o servidor usa um novo banco de dados (postgresql) para atender ao requisito de alta escalabilidade. Todas as informações de tarefa e de nó existente no banco de dados antigo (sqlite) são migradas para o novo banco de dados, exceto o histórico de tarefas e o log de atividades. Não é possível reverter para o banco de dados antigo (sqlite) após a migração.
- Após a migração, a saída é exibida em um formato diferente do comando d2djobhistory.
- Como prática recomendada, uma tarefa de backup deve fazer backup de menos de 1.000 nós.

Atualizar o arquivo de configuração TOMCAT

Ao atualizar o Agente do Arcserve UDP (Linux) de uma versão anterior, por exemplo, a r16.5 SP1, atualize o arquivo de configuração TOMCAT para atender ao requisito de alta escalabilidade do servidor de backup. Esta atualização permite que você faça backup de mais de 200 nós usando um servidor de backup.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá até a pasta bin:

   ```
   /opt/Arcserve/d2dserver/bin
   ```

3. Verifique se não há tarefas em execução e, em seguida, pare o servidor de backup usando o seguinte comando:

   ```
   ./d2dserver stop
   ```

   Se houver tarefas em execução, aguarde a conclusão das tarefas antes da interrupção do servidor de backup.

   ```
   /opt/Arcserve/d2dserver/TOMCAT/conf/
   ```

4. Atualize os seguintes parâmetros.

   Se o https for usado, atualize os seguintes parâmetros:

   ```
   <Connector port="8014" connectionTimeout="180000" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="300" acceptCount="200" scheme="https" secure="true" clientAuth="false" sslProtocol="TLSv1, TLSv1.1, TLSv1.2" keystoreFile="${catalina.home}/conf/server.keystore keystorePass="LinuxD2D"/>
   ```

   Se o http for usado, atualize os seguintes parâmetros:

   ```
   <Connector connectionTimeout="180000" port="8014" maxThreads="300" acceptCount="200" protocol="HTTP/1.1"/>
   ```

   O arquivo de configuração TOMCAT foi atualizado com êxito.

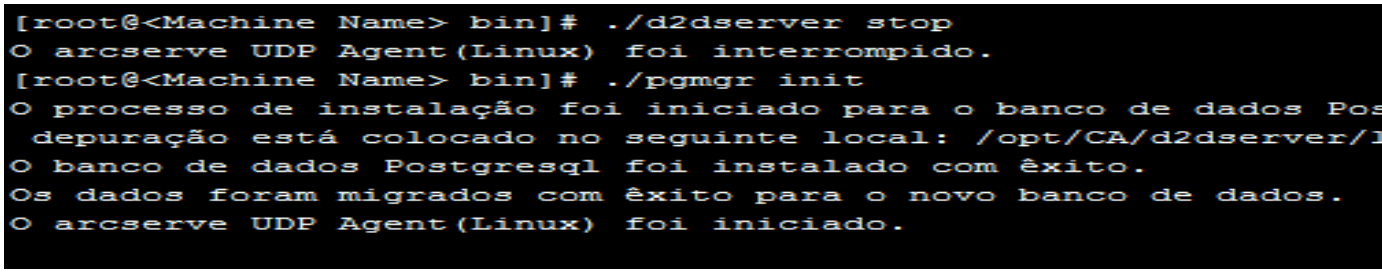
5. Interromper o servidor de backup.

   ```
   ./d2dserver stop
   ```

6. Execute o comando a seguir para iniciar o servidor de backup:

   ```
   ./pgmgr init
   ```

O comando verifica se todas as alterações necessárias foram concluídas e inicia o servidor de backup.



O servidor de backup e o servidor de banco de dados são iniciados com êxito.

Gerenciar o servidor de banco de dados

O comando *d2dserver start* geralmente inicia o servidor de banco de dados junto com o servidor de backup. Se não houver tarefas em andamento, o comando *d2d-server stop* em geral interrompe os dois servidores.

Se desejar iniciar e parar o servidor de banco de dados manualmente, será possível executar os seguintes comandos:

pgmgr start

Inicia o servidor de banco de dados.

pgmgr stop

Interrompe o servidor de banco de dados.

pgmgr status

Exibe o status do servidor de banco de dados. Será exibido se o servidor de banco de dados estiver em execução ou estiver parado.

Observação: se o banco de dados estiver carregado com excesso de dados, o console do Agente do Arcserve UDP (Linux) demorará mais tempo para carregar dados para o histórico de tarefas e para o log de atividades. Para melhorar a consulta de dados, consulte Melhorar o desempenho da consulta do histórico de tarefas e do log de atividades.

Adicionar nós Linux para backup

Adicione nós Linux, de modo que você possa fazer backup desses nós para um local de armazenamento de backup. Os nós Linux são os computadores do quais você deseja fazer backup. É possível adicionar nós manualmente ou executar um script para detectar e adicionar nós.

Siga estas etapas:

1. Digite o URL do servidor de backup em um navegador para abrir a interface do usuário.

   Observação: durante a instalação do agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor.

2. Execute as tarefas a seguir se você desejar detectar nós usando um script:

   a. Clique em Adicionar no menu Nó e selecione Detecção.

      A caixa de diálogo Detecção do nó abre.

   b. Selecione um script na lista suspensa Script.

      Observação: para obter mais informações sobre como criar o script de detecção de nós, consulte Detectar nós usando um script em Como integrar e automatizar o agente do Arcserve UDP (Linux) com o ambiente de TI existente.

   c. Especifique a Programação e clique em OK.

      A caixa de diálogo Detecção do nó é fechada, e o processo de detecção do nó é iniciado. A guia Log de atividades é atualizada com uma nova mensagem.

3. Execute as tarefas a seguir se desejar adicionar cada nó manualmente:

   a. Clique em Adicionar no menu Nó e selecione Nome do host/Endereço IP.

      A caixa de diálogo Adicionar nó é aberta.

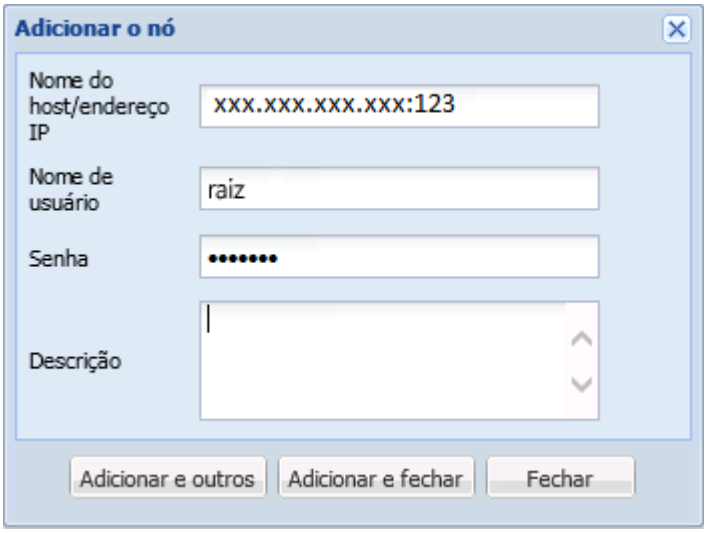
   b. Digite o nome do host ou o endereço IP do nó Linux, o nome de usuário que tenha a permissão raiz e a senha.

      Observação: se a porta SSH padrão do nó for alterada, será possível adicionar o nó da seguinte maneira:

      `<IP Name>: número da porta`

      Exemplo: xxx.xxx.xxx.xxx:123

      Onde, xxx.xxx.xxx.xxx é o endereço IP e 123 é o número da porta.



c. (Opcional) Digite uma descrição para o nó para ajudá-lo a localizar o nó.

d. Selecione uma das seguintes opções.

Adicionar e outros

Permite adicionar vários nós, um de cada vez. Após terminar de adicionar os nós, clique em Adicionar e fechar ou em Fechar para fechar a caixa de diálogo Adicionar o nó.

Adicionar e fechar

Permite que você adicione um nó e, em seguida, a caixa de diálogo Adicionar o nó é fechada.

Fechar

Fecha a caixa de diálogo sem adicionar nós.

4. Clique na guia Nós e verifique se novos nós estão listados nela.

   Os nós Linux são adicionados ao backup.

(Opcional) Registrar a chave pública do Arcserve UDP para inicialização segura

Ao ser executado em Inicialização segura, o nó de origem do backup precisa da instalação manual da chave pública do Arcserve para que o driver do backup seja confiável. Somente quando a chave está registrada, o recurso de backup e gerenciamento do nó funciona corretamente. Este tópico descreve como registrar a chave pública do Arcserve para o nó ativado por Inicialização segura.

Pré-requisitos:

- Verifique se você tem acesso à chave pública do Arcserve.
- Verifique se o seu sistema possui o pacote associado do arquivo MokManager.efi, que está localizado na pasta a seguir:

  RedHat: pasta /boot/efi/EFI/redhat

  CentOS: /boot/efi/EFI/centos

  Ubuntu: /boot/efi/EFI/ubuntu

  SLES: /boot/efi/EFI/SLES12

Siga estas etapas:

1. Efetue logon no ambiente do shell do nó de origem do backup.
2. Encontre a chave pública do Arcserve no seguinte local:

   `/tmp/arcserve_public_key_for_secureboot.der`
3. No documento de distribuição do Linux em execução para adicionar a chave pública à lista MOK do UEFI, execute as seguintes etapas explicadas de acordo com o exemplo a seguir:

   a. Importe o certificado para MOK:

      mokutil [--root-pw] --import

      `/tmp/arcserve_public_key_for_secureboot.der`

      A opção --root-pw permite o uso direto do usuário-raiz. A senha-raiz é obrigatória para registrar a chave após reinicializar o sistema.

   b. Especifique uma senha para o certificado quando a opção --root-pw não estiver disponível.

      Essa senha é obrigatória para registrar a chave após reinicializar o sistema.

   c. Verifique a lista de certificados que estão preparados para serem registrados no mokutil:

mokutil --list-new>

A lista deve ter uma chave pública do Arcserve.

d. Reinicie o sistema.

O sistema executa a ferramenta de gerenciamento de chaves do UEFI de correção.

Observação: se a ferramenta de gerenciamento de chaves do UEFI de correção não for iniciada, talvez o sistema não tenha o arquivo MokManager.efi.

e. Digite a senha que você especificou ao importar a chave pública do Arcserve para registrar o certificado na lista MOK.

f. Verifique se a chave recém-importada aparece registrada depois que o sistema é iniciado:

mokutil --list-enrolled

A lista deve ter uma chave pública do Arcserve.

4. Adicione ou faça backup do nó novamente para verificar se a chave pública do Arcserve foi registrada com êxito.

O nó ativado por Inicialização segura está pronto para ser protegido pelo agente do Arcserve UDP (Linux).

(Opcional) Registrar a chave pública do Arcserve UDP para o kernel do Oracle Linux UEK6 com ativação da inicialização segura

Esta seção fornece informações sobre como registrar a chave pública da Arcserve para o kernel do Oracle Linux UEK6 com ativação da inicialização segura.

Pré-requisitos:

- Verifique se você tem credenciais raiz.
- Verifique se você tem acesso à chave pública da Arcserve.
- Verifique se você tem acesso ao arquivo de chave da plataforma Arcserve (PKCS12).
- Verifique se o seu sistema tem o pacote associado ao arquivo **mmx64.efi**, que está localizado sob o caminho a seguir:

  /boot/efi/EFI/redhat

- Instale os seguintes pacotes, conforme necessário:

- Oracle Linux 7.x
  - *sudo yum install kernel-uek-devel*
  - *sudo yum update*
  - *sudo yum-config-manager –enable ol7_optional_latest*
  - *sudo yum install keyutils mokutil pesign*
- Oracle Linux 8.x
  - *sudo dnf install kernel-uek-devel*
  - *sudo dnf update*
  - *sudo dnf install keyutils mokutil pesign*

Siga estas etapas:

1. Efetue logon no ambiente do shell do nó de origem do backup.
2. Encontre a chave pública da Arcserve no seguinte local:

   `/tmp/arcserve_public_key_for_secureboot.der`
3. Localize o arquivo de chave da plataforma Arcserve (PKCS12) no seguinte local:

   `/tmp/arcserve_p12key_for_secureboot.p12`
4. Na documentação do Oracle Linux sobre como inserir o certificado do módulo no kernel e assinar a imagem do kernel UEK6, siga estas etapas:
   a. Para mudar para o diretório em que estão os arquivos de chave pública e da plataforma Arcserve, execute o seguinte comando:

      ```
      # cd /tmp
      ```

   b. Para inserir o certificado do módulo na imagem do kernel usando o utilitário *insert-sys-cert*, execute o seguinte comando:

      ```
      # /usr/src/kernels/$(uname -r)/scripts/insert-sys-cert -
      s /boot/System.map-$(uname -r) -z /boot/vmlinuz-$(uname
      -r) -c arcserve_public_key_for_secureboot.der
      ```

   c. Para configurar o banco de dados NSS, que é projetado para armazenar um conjunto completo de chaves, execute o seguinte comando:

      ```
      # certutil -d . -N

      Enter a password which will be used to encrypt your keys.
      The password should be at least 8 characters long,
      and should contain at least one non-alphabetic character.

      Enter new password:
      Re-enter password:
      ```

Você será solicitado a digitar uma senha para o banco de dados NSS. Digite uma senha para o banco de dados, que é necessária ao assinar o kernel.

d. Adicione a versão PKCS#12 da chave de assinatura do kernel ao novo banco de dados. Em primeiro lugar, será solicitada a senha do banco de dados NSS criado na etapa acima e, em seguida, será solicitada a senha usada durante a exportação do arquivo de chave PKCS#12 (cad2d é a senha usada para a chave PKCS#12).

 # pk12util -d . -i arcserve_p12key_for_secureboot.p12

```
Enter Password or Pin for "NSS Certificate DB":
Enter password for PKCS12 file:
pk12util: PKCS12 IMPORT SUCCESSFUL
```

e. Assine a imagem do kernel usando o utilitário pesign.

```
# pesign -u 0 -i /boot/vmlinuz-$(uname -r) --remove-signature -o vmlinuz.unsigned
# pesign -n . -c cert -i vmlinuz.unsigned -o vmlinuz.signed -s
Enter Password or Pin for "NSS Certificate DB":

# cp -bf vmlinuz.signed /boot/vmlinuz-$(uname -r)
```

5. Para atualizar o banco de dados MOK, siga estas etapas:

a. Para importar a certificação para o MOK, execute o seguinte comando:

mokutil [--root-pw] --import

/tmp/arcserve_public_key_for_secureboot.der

A opção --root-pw permite o uso do usuário raiz. A senha raiz é obrigatória para registrar a chave após reinicializar o sistema.

b. Especifique uma senha para o certificado quando a opção --root-pw não estiver disponível.

Essa senha é obrigatória para registrar a chave após reinicializar o sistema.

c. Verifique a lista de certificados que estão preparados para serem registrados no mokutil com o seguinte comando:

mokutil --list-new>

A lista deve incluir uma chave pública da Arcserve.

d. Reinicie o sistema.

O sistema executa a ferramenta de gerenciamento de chaves do UEFI de correção.

Observação: se a ferramenta de gerenciamento de chaves do UEFI de correção não for iniciada, talvez o sistema não tenha o arquivo *mmx64.efi*.

e. Digite a senha que você especificou ao importar a chave pública da Arcserve para registrar o certificado na lista do MOK.

6. Para o UEK R6, somente as chaves listadas no conjunto de chaves *builtin_trusted_keys* do kernel são confiáveis para a assinatura do módulo. Por esse motivo, as chaves de assinatura do módulo são adicionadas à imagem do kernel como parte do processo de assinatura dos módulos. Execute o seguinte comando para validar se uma chave é confiável:

   # keyctl show %:.builtin_trusted_keys

   Keyring: *335047181 ---lswrv 0 0 keyring: .builtin_trusted_keys*

   1042239099 ---lswrv 0 0 _ asymmetric: Oracle CA Server: *58bd7e-a9c4fba3a4a62720d5d06f1e96053ddf4d*

   24285436 ---lswrv 0 0 _ asymmetric: Arcserve kernel module signing key: *fb4c19d-ca60d31bb203499bf6cb384af6615699d*

   362335717 ---lswrv 0 0 _ asymmetric: Oracle America, Inc.: Ksplice Kernel Module Signing Key: *09010ebef5545fa7c54b626ef518e077b5b1ee4c*

   448587676 ---lswrv 0 0 _ asymmetric: Oracle Linux Kernel Module Signing Key: *2bb352412969a3653f0eb6021763408ebb9bb5ab*

   Observações:

   - A lista deve incluir uma chave pública da Arcserve.
   - Se vários kernels da versão do UEK estiverem instalados, a assinatura de apenas um kernel não permitirá o logon de outros kernels. Por exemplo, se você tiver instalado os kernels UEK5 e UEK6, importado uma chave e assinado o kernel UEK6 usando as etapas acima, a inicialização segura usando o kernel UEK5 falhará.

   O kernel do Oracle Linux UEK6 ativado para inicialização segura está pronto para proteção.

(Opcional) Preparar o volume iSCSI como o armazenamento de backup

É possível armazenar seus pontos de recuperação em um volume do iSCSI (Internet Small Computer System Interface). O iSCSI é usado para gerenciar a transferência de dados e o armazenamento em uma rede usando o IP padrão.

Verifique se você tem a release mais recente do software iniciador iSCSI instalada no servidor de backup. O software iniciador em sistemas RHEL é empacotado como iscsi-initiator-utils. O iniciador de software em sistemas SLES é empacotado como open-iscsi.

Siga estas etapas:

1. Efetue logon no ambiente do shell do nó de origem do backup.
2. Execute um dos comandos a seguir para iniciar o daemon do iniciador iSCSI.
   - Para sistemas RHEL:

     ```
     /etc/init.d/iscsid start
     ```

     O serviço em sistemas RHEL é denominado iscsid
   - Para sistemas SLES:

     ```
     /etc/init.d/open-iscsi start
     ```

     O serviço em sistemas SLES é denominado open-iscsi.
3. Execute um script de detecção para detectar o host de destino iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   O valor da porta padrão do host de destino iSCSI é 3260.
4. Anote o IQN (iSCSI Qualified Name – Nome Qualificado iSCSI) do host de destino iSCSI encontrado pelo script de detecção antes de efetuar logon manualmente no destino detectado.
5. Liste o dispositivo de bloqueio disponível do nó de origem do backup.

   ```
   #fdisk -l
   ```
6. Efetue logon no destino detectado.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>  -l
   ```

   É possível ver um dispositivo de bloco no diretório /dev do nó de origem do backup.

7. Execute o comando a seguir para obter o novo nome do dispositivo:

   ```
   #fdisk –l
   ```

   É possível ver um dispositivo adicional nomeado /dev/sd<x> no nó de origem do backup.

   Por exemplo, considere que o nome do dispositivo é /dev/sdc. Esse nome de dispositivo é usado para criar uma partição e um sistema de arquivos nas etapas abaixo.

8. Formate e monte o volume iSCSI.
9. Crie uma partição e um sistema de arquivos no nó de origem de backup usando os comandos a seguir.

   ```
   # fdisk /dev/sdc
   ```

   Se você tiver criado apenas uma partição, use o seguinte comando para criar um sistema de arquivos para uma única partição:

   ```
   # mkfs.ext3 /dev/sdc1
   ```

10. Monte a nova partição usando os seguintes comandos:

    ```
    # mkdir /iscsi
    # mount /dev/sdc1 /iscsi
    ```

    A nova partição é montada e o volume iSCSI fica pronto para ser usado como um armazenamento de backup em uma tarefa de backup.

11. (Opcional) Adicione o seguinte registro à pasta /etc/fstab de maneira que o volume iSCSI se conecte automaticamente ao servidor de backup após reiniciar o servidor.

    ```
    /dev/sdc1 /iscsi ext3 _netdev 0 0
    ```

    O volume iSCSI está pronto para ser usado como o armazenamento de backup.

Definir as configurações de backup e executar a tarefa de backup

Defina as configurações de backup usando o Assistente de backup. É possível fazer backup de seus dados para um local do NFS, um NAS (Network-Attached Storage – Armazenamento Anexado à Rede), um CIFS ou para um local de origem. Um local de origem é um local no nó de backup de origem no qual os dados do backup estão armazenados. O processo de backup é iniciado por uma tarefa de backup. O Assistente de backup cria a tarefa de backup e a executa. Cada vez que você executa um backup com êxito, um ponto de recuperação é criado. Um ponto de recuperação é uma cópia pontual do nó de backup.

Especifique a Origem do backup

Especifique os nós de origem do backup no Assistente de backup de modo que você possa fazer backup desses nós em um local desejado. A página Origem do backup do Assistente de backup exibe o nó que você deseja incluir no backup. Use o botão Adicionar dessa página para adicionar mais nós para backup.

Observação: se você abrir o Assistente de backup usando o botão Fazer backup dos nós selecionados, todos os nós selecionados serão listados na página do assistente. Se você abrir o Assistente de backup usando o botão Fazer backup, os nós não serão listados na página do assistente. É necessário adicionar nós usando o botão Adicionar na página do assistente.

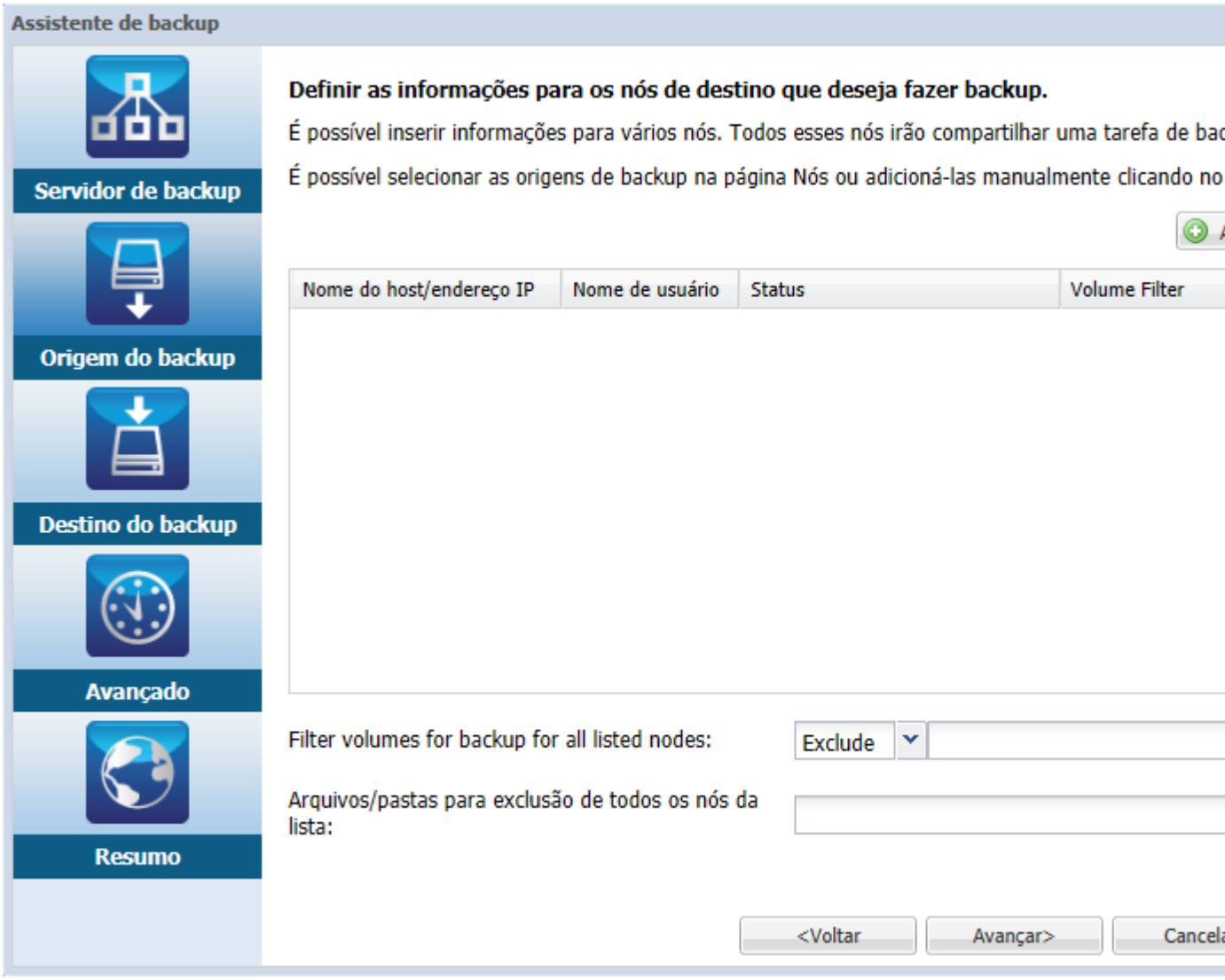
Siga estas etapas:

1. Selecione os nós dos quais deseja fazer backup na guia Nós.
2. Clique em Fazer backup e selecione a opção Fazer backup dos nós selecionados no menu Assistente.

   A página do servidor de backup do Assistente de backup é exibida. A página do servidor de backup exibe o nome do servidor.

3. Clique em Avançar.

   A página Origem do backup é exibida. Os nós selecionados anteriormente são exibidos nessa página.



4. (Opcional) Clique em Adicionar na página Origem do backup para adicionar mais nós e fornecer os detalhes na caixa de diálogo Adicionar o nó.
5. (Opcional) Insira os volumes em **Volumes a serem filtrados para todos os nós listados**.

   Na lista suspensa, selecione Incluir ou Excluir. Incluir especifica que apenas os volumes especificados serão incluídos no backup. Não será feito backup de qualquer volume que não for especificado. Excluir especifica que os volumes serão excluídos do backup.
6. (Opcional) Insira os arquivos/pastas em **Arquivos/pastas a serem excluídos de todos os nós listados**.

   Os arquivos/pastas devem ser especificados com um nome de caminho absoluto e separados por dois-pontos (:). Os caracteres curinga como * e ? são suportados e

devem ser usados após a última barra do nome de caminho absoluto. Se o nome dos arquivos/pastas após a última barra estiver entre parênteses, esses arquivos/pastas serão excluídos de forma recursiva. Caso contrário, os arquivos/pastas serão excluídos diretamente.

Por exemplo:

`/home/user/a/foo*:/home/user/b/(foo*)`

A primeira parte (home/user/a/foo*) excluirá somente os arquivos/pastas que correspondem a foo* em "/home/user/a", mas fará backup de subdiretórios de dentro. A segunda parte (/home/user/b/(foo*) excluirá todos os arquivos/pastas que correspondem a foo* em "/home/user/b", bem como todas as suas subpastas.

Observações:

- Se muitos arquivos/pastas forem excluídos de um volume, será recomendável excluir o volume em questão.
- Se muitos arquivos/pastas forem excluídos, a fase da tarefa e o status poderão permanecer "Fazendo backup do volume" e "Ativo" por um longo período, quando a tarefa de backup é iniciada.
- Se o valor **Arquivos/pastas para exclusão de todos os nós da lista** for alterado, a tarefa de backup será convertida em um backup completo.

Se determinados arquivos de sistema forem excluídos do backup, o Linux OS poderá não ser inicializado e a função BMR não funcionará corretamente. Esses arquivos de sistema incluem, entre outros:

- Arquivos e pastas em /bin, /sbin, /usr, /etc, /lib, /lib64, /boot, /var
- Pasta /proc, /sys, /dev, /tmp

Se excluir os arquivos do sistema, será recomendável verificar a função BMR e confirmar se o Linux OS será inicializado corretamente.

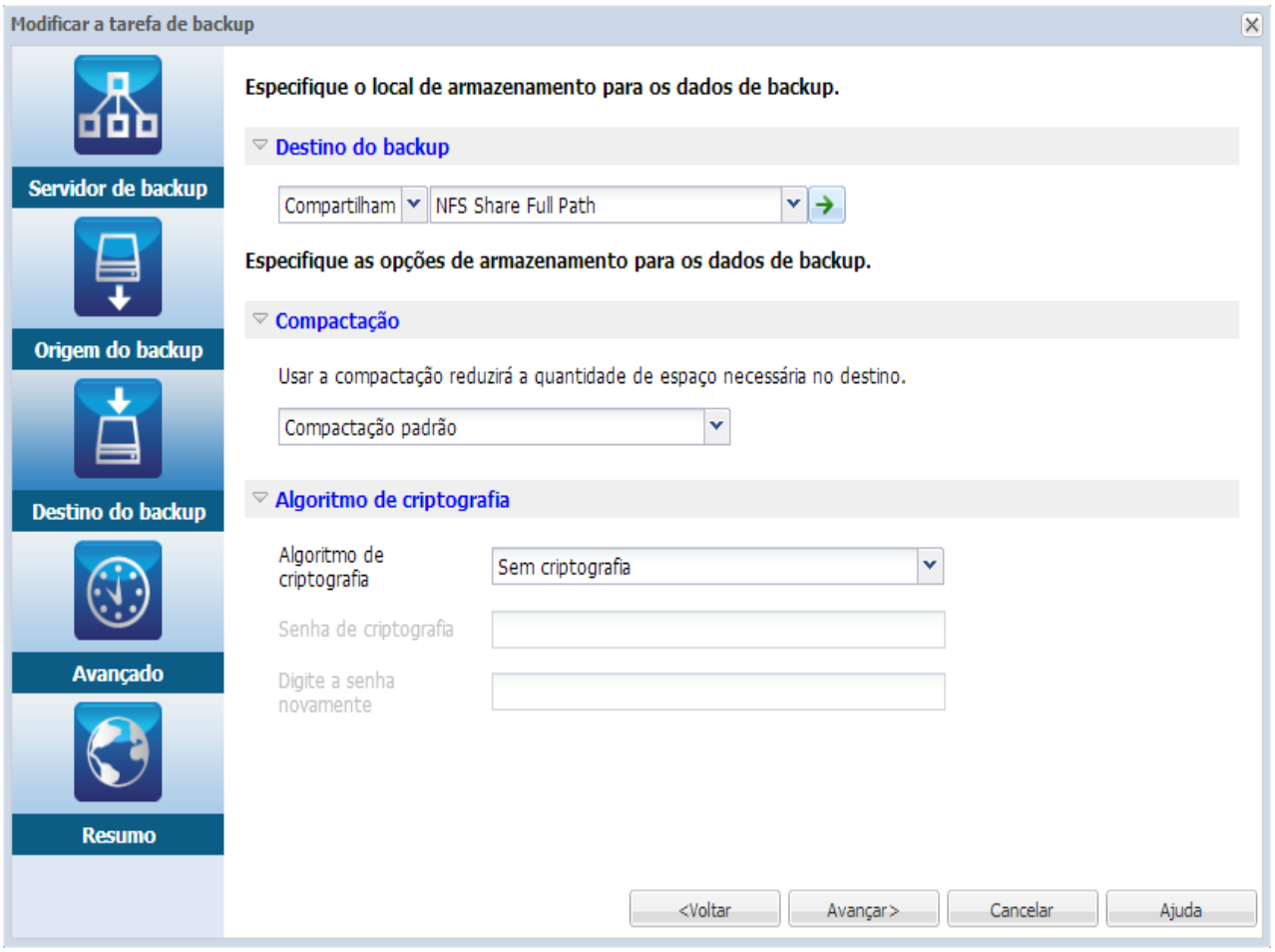
7. Clique em Avançar.

   A página Destino do backup é exibida.

   A origem do backup é especificada.

Especifique o Destino do backup

Especifique um local para armazenar os dados de backup (pontos de recuperação) na página Destino do backup do Assistente de backup. O destino do backup pode ser um compartilhamento NFS, compartilhamento CIFS ou um local de origem. O local de origem é o nó de origem do backup. Se o destino de backup for o local de origem, os dados de backup serão gravados em seu próprio disco local diretamente.



Se o disco físico incluir dois volumes lógicos, você pode especificar um volume como a origem do backup e o outro como o destino.

Observação: se você selecionar Local de origem como destino de backup, o servidor de backup não poderá gerenciar os pontos de recuperação. Para gerenciar os conjuntos de recuperação, consulte Gerenciar os conjuntos de recuperação em Como gerenciar as configurações do servidor de backup.

Siga estas etapas:

1. Selecione um destino da lista suspensa Destino do backup e insira o caminho completo do local de armazenamento.

- Se tiver selecionado Compartilhamento NFS, digite os detalhes do destino de backup no seguinte formato:

  `IP_address_of_the_NFS_Share:/full_path_of_the_storage_location`

  Observação: algumas versões do Domínio de dados do NAS não oferecem suporte ao mecanismo de bloqueio de arquivos do NFS. Como resultado, esse compartilhamento do NFS não pode ser usado como destino de backup. Para obter mais informações sobre esse problema, consulte Problemas de compatibilidade com o Agente do Arcserve UDP (Linux) em Notas da Versão.

- Se tiver selecionado Compartilhamento CIFS, digite os detalhes do destino de backup no seguinte formato:

  `//nomehost/pasta_compartilhamento`

  Observação: o nome da pasta compartilhada não pode conter nenhum espaço.

- Se tiver selecionado Local de origem, será necessário modificar algumas configurações para que o servidor de backup possa gerenciar os pontos de recuperação. Por exemplo, considere servidor A como o nome do host do servidor de backup e nó B como o nome do host do nó de origem. Agora, siga estas etapas para modificar as configurações do node-B:
  - Verifique se o servidor do NFS está sendo executado. É possível executar o seguinte comando para verificar o status do servidor do NFS:

    service nfs status

  - Se o servidor do NFS não estiver em execução, execute o seguinte comando para iniciar o servidor do NFS:

    service nfs start

  - Se sua pasta de destino do backup em node-B for */backup/teste*, adicione a seguinte linha a */etc/exportações*:

    /backup/test server-A(rw,no_root_squash)

    Agora, execute o seguinte comando:

    exportfs -a

  - Na interface do usuário do servidor de backup, adicione *node-B:/backup/teste* como um local de repositório de backup. O local de armazenamento do local de origem é exibido na lista suspensa Destino do backup.

- Se você tiver selecionado Amazon S3, digite os detalhes do destino de backup no seguinte formato:

  //ID_da_região_do_S3/Nome_do_compartimento_de_memória_do_S3

  Observações:

  - //./ pode ser usado como atalho para a conta global do Amazon. Por exemplo, //./Global_bucket_name
  - //China/ pode ser usado como atalho para a conta da China na nuvem do Amazon. Por exemplo, //China/Nome_do_compartimento_de_memória_da_China
  - Se você quiser exportar o compartimento de memória do Amazon S3 como um compartilhamento CIFS, poderá clicar na caixa de seleção Ativar acesso para clientes CIFS. A porta padrão é 8017.

    Esse recurso tem o seguinte arquivo de configuração:

    /opt/Arcserve/d2dserver/configfiles/ofs.cfg

    Não modifique o conteúdo original dele. Você pode adicionar o conteúdo abaixo:

    - PROXY_HOST= (se desejar usar o proxy, insira aqui o nome do proxy.)
    - PROXY_USERNAME= (nome de usuário do proxy)
    - PROXY_PASSWORD_ENC= (senha do proxy, que deve ser criptografada)
    - PROXY_PORT= (porta do proxy)
    - WRITE_THROUGHPUT= (se desejar limitar a taxa de transferência de gravação, Unidade: KB/s)
    - HTTPS = sim/não (o padrão é sim)
    - S3_STORAGE_CLASS = STANDARD/STANDARD_IA/REDUCED_REDUNDANCY (o padrão é STANDARD)
    - DEBUG_LEVEL= (nível do log de depuração: 0,1,2,3, 3 imprimirá a maioria dos logs)

2. Clique no botão de seta para validar as informações do destino do backup.

   Se o destino do backup for inválido, uma mensagem de erro será exibida.

3. Selecione um nível de compactação da lista suspensa Compactação para especificar um tipo de compactação a ser usado para o backup.

As opções disponíveis para Compactação são:

Compactação padrão

Especifica que essa opção proporciona um bom equilíbrio entre o uso da CPU e o uso do espaço em disco. Essa compactação é a configuração padrão.

Compactação máxima

Especifica que essa opção proporciona maior uso da CPU (menor velocidade), mas também menos uso de espaço em disco para sua imagem de backup.

4. Selecione um algoritmo na lista suspensa Algoritmo de criptografia e digite a senha de criptografia, se necessário.
   a. Selecione o tipo de algoritmo de criptografia que deseja usar para os backups.

      A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A proteção de dados do Agente do Arcserve UDP (Linux) usa algoritmos seguros de criptografia AES (Advanced Encryption Standard) para atingir o máximo de segurança e privacidade dos dados especificados.

      As opções de formatação são Sem criptografia, AES-128, AES-192 e AES-256. (Para desativar criptografia, selecione Sem criptografia.)

      - Um backup completo e todos os seus backups incrementais relacionados devem usar o mesmo algoritmo de criptografia.
      - Se o algoritmo de criptografia para um backup incremental foi alterado, é necessário executar um backup completo.

        Por exemplo, se você alterar o formato do algoritmo e, em seguida, executar um backup incremental, o tipo de backup é convertido automaticamente para um backup completo.

   b. Quando um algoritmo de criptografia é selecionado, você deve fornecer (e confirmar) uma senha de criptografia.
      - A senha de criptografia é limitada a um máximo de 23 caracteres.
      - Um backup completo e todos os seus backups incrementais relacionados utilizam a mesma senha para criptografar dados.
5. Clique em Avançar.

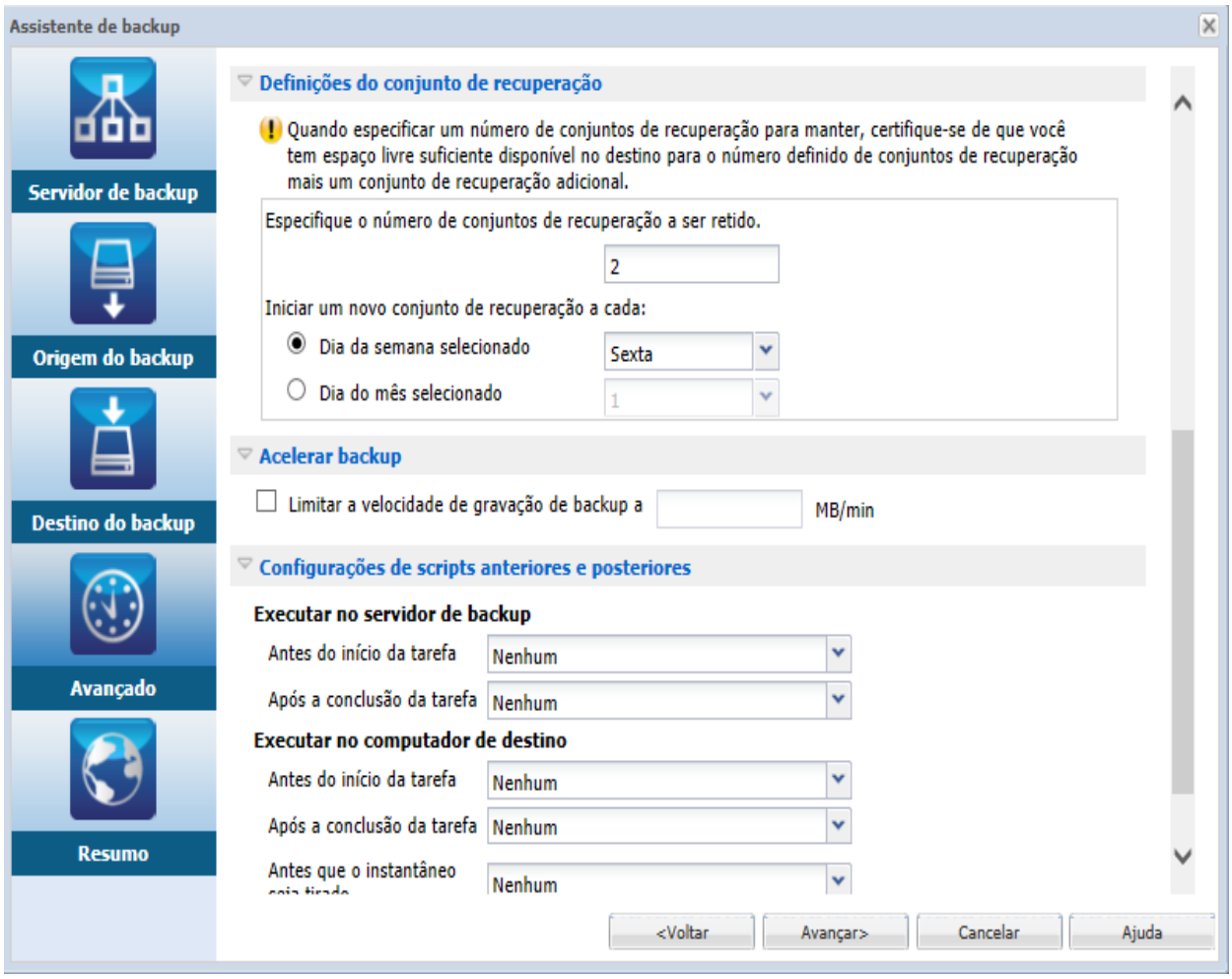
   A página Avançado é exibida.

O destino do backup é especificado.

Especificar as configurações avançadas

Especifique a programação de backup, as definições do conjunto de recuperação e as configurações pré-backup e pós-backup na página Avançado.

O diagrama a seguir exibe a página Avançado do Assistente de backup. Neste diagrama, a opção Nenhum é selecionada para o Tipo de programação.



As seguintes configurações estão disponíveis na página Avançado:

- As configurações de Programação garantem que a tarefa de backup seja executada periodicamente em horas especificadas.

  Importante: defina o mesmo fuso horário para o servidor UDP e o servidor de backup Linux. Depois de alterar o fuso horário nos dois servidores, é preciso reiniciar o serviço de gerenciamento do UDP ou o servidor de backup Linux para que as alterações entrem em vigor.

- As Definições do conjunto de recuperação garantem a manutenção periódica dos conjuntos de recuperação. Se o número de conjuntos de recuperação

exceder o número especificado, o conjunto de recuperação mais antigo será excluído para manter o número especificado todo o tempo.

- A configuração Acelerar backup permite ativar e especificar a velocidade máxima (MB/min) em que os backups são gravados.
- As Configurações de scripts anteriores e posteriores definem os scripts que podem ser executados no servidor de backup e no nó de destino. É possível configurar os scripts para executar ações específicas antes do início de uma tarefa, durante a execução da tarefa ou após a conclusão da tarefa.

Para otimizar o gerenciamento dos pontos de recuperação, você deve considerar as seguintes recomendações ao agendar a frequência dos backups:

- Para os sistemas protegidos com backups incrementais executados a cada 15 minutos, é recomendável agendar um backup completo a cada semana (para atualizar a imagem de base).
- Para os sistemas protegidos com backups incrementais executados a cada hora, é recomendável agendar um backup completo a cada mês (para atualizar a imagem de base).

Observação: se a quantidade de espaço usada para o armazenamento de imagens de backup for uma preocupação, você deve considerar a programação de backups completos com menos frequência para usar menos espaço de armazenamento.

Siga estas etapas:

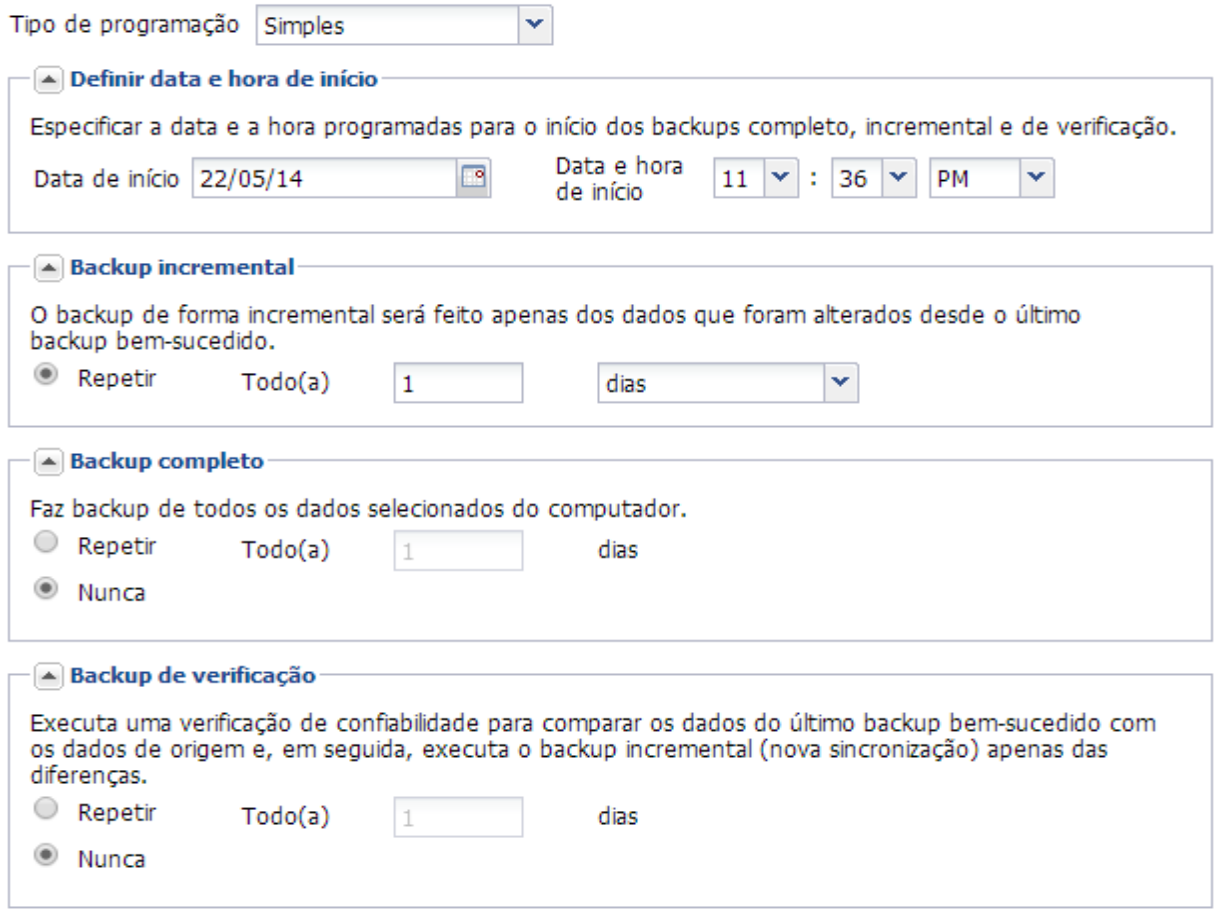
1. Defina a data e hora de início selecionando uma das opções a seguir na lista suspensa Tipo de programação:

Simples

O tipo de programação **Simples** não estará disponível quando você criar uma nova programação. No entanto, se você estiver modificando uma antiga tarefa de backup que tinha a programação simples, é possível configurar a programação simples.

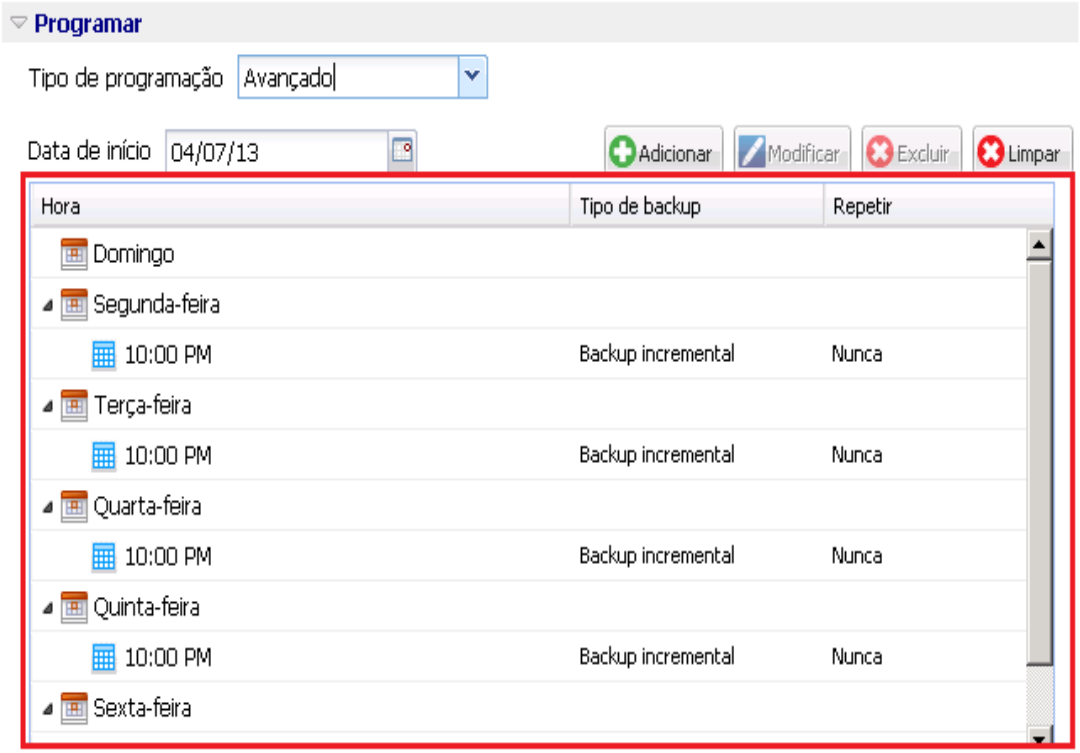
Selecione a opção Simples para programar o Backup incremental, Backup completo e Backup de verificação pela Data de início e Hora de início especificadas. Para cada tipo de backup, também é possível especificar a duração de repetição de um backup ou nunca repetir um backup. A data e hora de início é fixa para todos os tipos de backup. Portanto, não é possível especificar uma data e hora de início diferente para diferentes tipos de backup.

Observação: para obter mais informações sobre os tipos de backup, consulte *Noções básicas sobre os tipos de backup*.



Personalizado

Selecione a opção Personalizado para especificar várias programações de backup a cada dia da semana. É possível especificar uma data e hora de início diferente para diferentes tipos de backup. É possível adicionar, modificar e limpar a Programação personalizada. Ao clicar em Limpar, todas as programações de backup personalizadas são excluídas da bandeja de programação avançada.

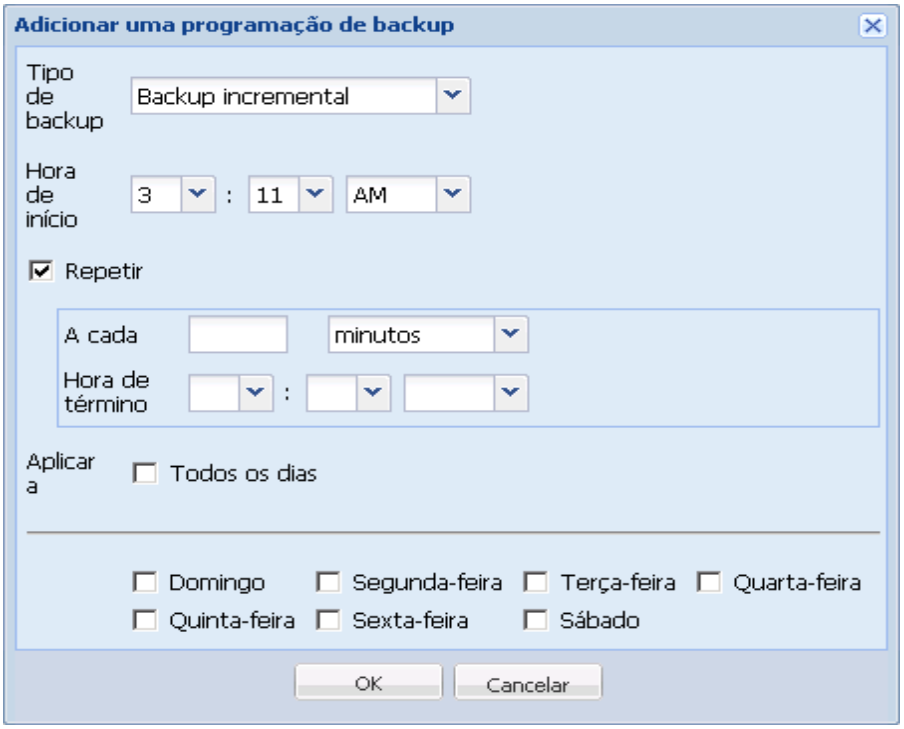


Programação avançada

Para adicionar uma programação de backup, siga estas etapas:

a. Clique em Adicionar.

A caixa de diálogo Adicionar uma programação de backup é aberta.



b. Especifique as opções de programação de backup e clique em OK.

A programação de backup especificada é exibida na Bandeja de programação personalizada.

Nenhum

Selecione a opção Nenhum para criar a tarefa de backup e armazenar a tarefa na guia Status da tarefa. Esta opção não irá executar a tarefa porque não há uma programação especificada. Ao enviar a tarefa, o status da tarefa muda para Pronto. Quando você deseja executar a tarefa, selecione a tarefa e clique em Executar agora no menu Tarefa. Cada vez que você deseja executar a tarefa, deve executar a tarefa manualmente. Também é possível criar um script para executar essa tarefa em sua própria programação personalizada.

2. Especifique as definições do conjunto de recuperação.

Observação: para obter mais informações sobre os conjuntos de recuperação, consulte *Noções básicas sobre os conjuntos de recuperação*.

Especifique o número de conjuntos de recuperação a ser retido

Especifica o número de conjuntos de recuperação retidos.

Iniciar um novo conjunto de recuperação a cada:

Dia da semana selecionado

Especifica o dia da semana selecionado para iniciar um novo conjunto de recuperação.

Dia do mês selecionado

Especifica o dia do mês selecionado para iniciar um novo conjunto de recuperação. Especifique de 1 a 30 ou o último dia do mês.

Observação: o servidor de backup verifica o número de conjuntos de recuperação no armazenamento de backup configurado a cada 15 minutos e exclui qualquer conjunto de recuperação extra do local de armazenamento de backup.

3. Especifique o valor Acelerar backup.

Você pode especificar a velocidade máxima (MB/min) em que os backups são gravados. É possível restringir a velocidade de backup para reduzir a utilização da CPU ou da rede. No entanto, ao limitar a velocidade de backup, isso terá um efeito negativo na janela de backup. À medida que se reduz a velocidade máxima do backup,

aumenta-se seu tempo de execução. No caso de uma tarefa de backup, a guia Status da tarefa exibe a velocidade média de leitura e gravação da tarefa em andamento e o limite de velocidade do acelerador configurado.

Observação: por padrão, a opção Acelerar backup não está ativada e a velocidade de backup não é controlada.

4. Especifique suas configurações de pré-backup e pós-backup nas Configurações de scripts anteriores e posteriores.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos Configurações de scripts anteriores e posteriores serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local:

   `/opt/Arcserve/d2dserver/usr/prepost`

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.

5. Clique em Avançar.

   A página Resumo é exibida.

   A programação personalizada é especificada.

   Observação: se em um determinado momento houver mais de um tipo de backup programado para execução simultânea, o tipo de backup que será executado terá como base as seguintes prioridades:

   - Prioridade 1 - Backup completo
   - Prioridade 2 - Backup de verificação
   - Prioridade 3 - Backup incremental

   Por exemplo, se você programar todos os três tipos de backup para serem executados ao mesmo tempo, o Agente do Arcserve UDP (Linux) executará o backup completo. Se não houver nenhum backup completo programado, mas você tiver programado um Backup de verificação e um Backup incremental para serem executados ao mesmo tempo, o Agente do Arcserve UDP (Linux) executará o Backup de verificação. Um backup incremental programado só será executado se não houver conflito com nenhum outro tipo de backup.

Noções básicas sobre os tipos de backup

É possível especificar os seguintes tipos de backup na página Avançado do Assistente de backup:

Backup incremental

Faz backup apenas daqueles blocos que foram alterados desde o último backup realizado com êxito. As vantagens do backup incremental são a rapidez e o tamanho reduzido da imagem de backup gerada. O Arcserve UDP para Linux usa um driver para monitorar os blocos que foram alterados no nó de origem após o último backup com êxito.

As opções disponíveis são Repetir e Nunca. Se selecionar a opção Repetir, é preciso especificar também o tempo decorrido (em minutos, horas, dias) entre as tentativas de backup.

Mínimo: 15 minutos

Padrão: 1 dia

Backup completo

Faz backup de todo o nó de origem. Dependendo do tamanho do volume do nó de backup, o backup completo gera uma imagem de backup grande e normalmente leva um tempo mais longo para ser concluído. As opções disponíveis são Repetir e Nunca.

Se selecionar a opção Repetir, é preciso especificar também o tempo decorrido (em minutos, horas, dias) entre as tentativas de backup.

Mínimo: 1 dia

Padrão: nunca (nenhuma repetição programada)

Verificar backup

Verifica se os dados protegidos são válidos e estão completos realizando uma verificação de confiabilidade da imagem de backup armazenada com a origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de algum bloco não corresponder à origem (possivelmente devido a alterações no sistema após o último backup), o Arcserve UDP para Linux atualizará (ressincronizará) o backup do bloco divergente. É possível também usar um backup de verificação (muito raramente)

para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

As opções disponíveis são Repetir e Nunca. Se selecionar a opção Repetir, é preciso especificar também o tempo decorrido (em minutos, horas, dias) entre as tentativas de backup.

Mínimo: 1 dia

Padrão: nunca (nenhuma repetição programada)

O tipo de backup que é executado depende das seguintes situações:

- Se você executar a tarefa de backup pela primeira vez para os nós selecionados, o primeiro backup será sempre um Backup completo.
- Se você executar a tarefa de backup novamente para o mesmo conjunto de nós e o destino de backup também for mesmo, o tipo de backup será Backup incremental.
- Se você executar a tarefa de backup para o mesmo conjunto de nós e o destino de backup for diferente, o tipo de backup será Backup completo. Isso ocorre porque você alterou o destino do backup e nesse novo destino é o primeiro backup. Portanto, o primeiro backup é um Backup completo.
- Se você excluir o nó e, em seguida, adicionar o mesmo nó novamente, mas não alterar o destino do backup, o backup será um Backup de verificação. Isso ocorre porque você já fez backup desse nó com as tarefas de backup anteriores. Quando você exclui o nó e, em seguida, adiciona o nó novamente, a tarefa de backup verifica todos os blocos desse nó com a última imagem de backup. Quando a tarefa de backup determina que é o mesmo nó, é feito backup apenas dos blocos alterados. Se a tarefa de backup não encontrar nenhuma imagem de backup desse nó no destino do backup, o tipo de backup será um Backup completo.

Noções básicas sobre os conjuntos de recuperação

Um conjunto de recuperação é uma configuração de armazenamento em que um grupo de pontos de recuperação obtidos em backup por período determinado é armazenado como um único conjunto. Um conjunto de recuperação é uma série de backups, iniciando com um backup completo e seguido de alguns backups incrementais, de verificação ou completos. É possível especificar o número de conjuntos de recuperação a reter.

As Definições do conjunto de recuperação garantem a manutenção periódica dos conjuntos de recuperação. Quando o limite especificado é excedido, o conjunto de recuperação mais antigo é excluído. Os valores a seguir definem os conjuntos de recuperação padrão, mínimo e máximo no Agente do Arcserve UDP (Linux):

Padrão: 2

Mínimo: 1

Número máximo de conjuntos de recuperação: 100

O número máximo de pontos de recuperação (incluindo um backup completo): 1344

Observação: se desejar excluir um conjunto de recuperação para economizar espaço de armazenamento de backup, reduza o número de conjuntos retidos e o servidor de backup excluirá automaticamente o conjunto de recuperação mais antigo. Não tente excluir o conjunto de recuperação manualmente.

Conjunto de exemplo 1:

- Completo
- Incremental
- Incremental
- Verificar
- Incremental

Conjunto de exemplo 2:

- Completo
- Incremental
- Completo
- Incremental

Um backup completo é necessário para iniciar um novo conjunto de recuperação. O backup que inicia o conjunto será convertido automaticamente em um backup

completo, mesmo que não haja nenhum backup completo configurado ou programado para ser executado nesse momento. Depois que a configuração do conjunto de recuperação for alterada (por exemplo, alterando o ponto de partida do conjunto de recuperação, do primeiro backup de segunda-feira para o primeiro backup de quinta-feira), o ponto de partida dos conjuntos de recuperação existentes não será alterado.

Observação: um conjunto de recuperação incompleto não é contado ao calcular um conjunto de recuperação existente. Um conjunto de recuperação é considerado concluído somente quando o backup inicial do próximo conjunto de recuperação é criado.

Exemplo 1 - Reter 1 conjunto de recuperação:

- Especifique o número de conjuntos de recuperação a serem retidos como 1.

  O servidor de backup sempre mantém dois conjuntos para manter um conjunto completo antes de iniciar o próximo conjunto de recuperação.

Exemplo 2 - Reter 2 conjuntos de recuperação:

- Especifique o número de conjuntos de recuperação a serem retidos como 2.

  O servidor de backup excluirá o primeiro conjunto de recuperação quando o quarto estiver pronto para iniciar a recuperação. Isso garante que, quando o primeiro backup for excluído e o quarto estiver sendo iniciado, você ainda tenha dois conjuntos de recuperação (conjunto de recuperação 2 e conjunto de recuperação 3) disponíveis no disco.

  Observação: mesmo que você opte por reter apenas um conjunto de recuperação, precisará de espaço para pelo menos dois backups completos.

Exemplo 3 - Reter 3 conjuntos de recuperação:

- A hora de início do backup é às 6h00 de 20 de agosto de 2012.
- Um backup incremental é executado a cada 12 horas.
- Um novo conjunto de recuperação começa no último backup na sexta-feira.
- Você deseja reter 3 conjuntos de recuperação.

Com a configuração acima, um backup incremental será executado às 6h00 e outro às 18h00, diariamente. O primeiro conjunto de recuperação é criado quando o primeiro backup (deve ser um backup completo) é realizado. Em seguida, o primeiro backup completo é marcado como o backup inicial do conjunto de recuperação. Quando o backup programado para as 18h de sexta-feira for executado, ele será

convertido em um backup completo e marcado como o backup inicial do conjunto de recuperação.

(Opcional) Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar seus scripts em **Configurações de scripts anteriores/posteriores** do **Assistente de backup** e do **Assistente de restauração** no console. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

Variáveis de ambiente de script anterior e posterior

Para criar seu script, use as seguintes variáveis de ambiente:

D2D_JOBNAME

Identifica o nome da tarefa.

D2D_JOBID

Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

D2D_TARGETNODE

Identifica o nó cujo backup está sendo feito ou restaurado.

D2D_JOBTYPE

Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

backup.full

Identifica a tarefa como um backup completo.

backup.incremental

Identifica a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino antes da conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino antes do início da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

D2D_RECOVERYPOINT

Identifica o ponto de recuperação criado pela tarefa de backup. Esse valor é aplicável no script de backup posterior somente.

D2D_RPSSCHEDULETYPE

Identifica o tipo de programação durante o backup para um repositório de dados no RPS. Os valores a seguir identificam a variável D2D_ RPSSCHEDULETYPE:

diário

Identifica a programação como um backup diário.

semanal

Identifica a programação como um backup semanal.

mensal

Identifica a programação como um backup mensal.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   `/opt/Arcserve/d2dserver/usr/prepost`

2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.
6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Executar a tarefa de backup

Execute a tarefa de backup para que um ponto de recuperação seja criado. É possível usar esse ponto de recuperação para restaurar os dados.

Na página Resumo, verifique o resumo dos detalhes de backup e forneça um nome de tarefa para diferenciá-la das outras tarefas.

Siga estas etapas:

1. Verifique o resumo e digite um nome de tarefa.

   O campo Nome da tarefa tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

2. (Opcional) Clique em Voltar para modificar qualquer configuração em qualquer página do assistente.
3. Clique em Enviar.

   O processo de backup é iniciado. Na guia Status da tarefa, a tarefa é adicionada e o status do backup será exibido.

   A tarefa de backup é criada e executada.

Verificar se o backup foi bem-sucedido

Após a conclusão da tarefa de backup, verifique se o ponto de recuperação foi criado no destino especificado.

Siga estas etapas:

1. Navegue até ao destino especificado no qual você tenha armazenado os dados de backup.
2. Verifique se os dados do backup estão presentes nesse destino.

   Por exemplo, se o nome da tarefa de backup for *Demo* e o destino de backup for xxx.xxx.xxx.xxx:/Dados, navegue até ao destino de backup e verifique se um novo ponto de recuperação é gerado.

   Os dados de backup são verificados com êxito.

   O backup dos nós Linux é feito com sucesso.

Como modificar e executar novamente uma tarefa de backup

Se você já tiver criado uma tarefa para um nó, será possível modificá-la e executar novamente a tarefa várias vezes. Não é necessário criar outra tarefa para proteger o mesmo nó. Se você não desejar fazer alterações na tarefa, também será possível executar a tarefa sem modificá-la. Modificar uma tarefa inclui adicionar um nó a uma tarefa existente, definindo as configurações da tarefa, ou ambos.

O diagrama a seguir mostra o processo para modificar e executar novamente uma tarefa de backup:

Execute estas tarefas para modificar e executar novamente uma tarefa de backup:

- Verificar os pré-requisitos para a modificação de uma tarefa de backup
- Deseja adicionar nós a uma tarefa existente?
- Adicionar nós a uma tarefa existente

- Executar novamente uma tarefa existente
- Verificar se o backup foi bem-sucedido

Verificar os pré-requisitos para a modificação de uma tarefa de backup

Verifique os seguintes requisitos antes de modificar e executar novamente uma tarefa de backup:

- Você tem uma tarefa de backup válida.
- Você adicionou os nós ao Arcserve UDP.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Deseja adicionar nós a uma tarefa existente?

Se você já tiver uma tarefa de backup e desejar proteger novos nós com as mesmas configurações de backup, será possível adicionar nós a uma tarefa existente. Depois de adicionar os nós, também é possível modificar as configurações de backup e executar a tarefa.

Adicionar nós a uma tarefa existente

É possível adicionar novos nós a uma tarefa de backup existente e executar a tarefa. Todas as configurações da tarefa selecionada são aplicadas ao novo nó, e não será necessário definir as novas configurações de backup. Use essa opção se desejar manter as mesmas configurações de backup para todos os nós.

Siga estas etapas:

1. Selecione todos os novos nós da guia Nós no painel Status.
2. No menu Assistente, clique em Fazer backup e selecioneAdicionar os nós selecionados em uma tarefa existente.

   A caixa de diálogo Adicionar os nós selecionados em uma tarefa existente é exibida.
3. Selecione uma tarefa na lista suspensa Nome da tarefa e clique em OK.

   O nó é adicionado à tarefa de backup selecionada e a coluna Protegido na guia Nós muda para Sim.

   Os nós são adicionados a uma tarefa existente.

Executar novamente uma tarefa de backup existente

Execute novamente a tarefa de backup para outro backup dos nós especificados. Um ponto de recuperação é criado depois de cada backup bem-sucedido. Se você já tiver feito o backup de um nó, não será necessário criar outra tarefa de backup para fazer backup desse nó novamente. Todas as tarefas anteriores são listadas na guia Status da tarefa no painel Status.

Ao executar novamente uma tarefa de backup, especifique o tipo da tarefa a ser executada novamente.

Observação: se você atualizar alguma informação na página Destino de backup do Assistente de backup antes de executar a tarefa, o tipo de tarefa será alterado automaticamente para *Backup completo*.

Siga estas etapas:

1. Digite o URL do Agente do Arcserve UDP (Linux) em um navegador para abrir a interface do usuário.

   Observação: durante a instalação do Agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor.

2. Clique na guia **Status da tarefa** e selecione a tarefa que deseja executar.
3. Verifique se o status da tarefa selecionada é Concluído ou Pronto.

   Concluído indica que a tarefa não está programada e Pronto indica que a tarefa está agendada.

4. Execute uma das seguintes etapas:
   - Para executar a tarefa sem alterações, faça o seguinte:

   a. Clique em **Executar agora** no menu Tarefa.

      A caixa de diálogo Executar a tarefa de backup agora é exibida.

   b. Selecione o Tipo de backup.

   c. Selecione uma opção na lista suspensa Executar tarefa para:

      Nó selecionado

      Especifica que a tarefa de backup é executada apenas para o nó selecionado.

      Todos os nós protegidos pela tarefa selecionada

      Especifica que a tarefa de backup é executada para todos os nós protegidos pela tarefa selecionada.

d. Clique em **OK**.

   A caixa de diálogo Executar a tarefa de backup agora é fechada. O status da tarefa muda para Ativo na guia Status da tarefa, e a mesma tarefa é executada novamente.

- Para modificar a tarefa antes de executá-la, siga estas etapas:

a. Selecione uma tarefa e clique em **Modificar**.

   A caixa de diálogo Executar a tarefa de backup agora é exibida.

b. Atualize o campo obrigatório no Assistente de backup.

c. Clique em **Enviar**.

   A tarefa será executada novamente de acordo com a programação da tarefa.

A tarefa de backup é executada novamente com êxito.

Verificar se o backup foi bem-sucedido

Após a conclusão da tarefa de backup, verifique se o ponto de recuperação foi criado no destino especificado.

Siga estas etapas:

1. Navegue até ao destino especificado no qual você tenha armazenado os dados de backup.
2. Verifique se os dados do backup estão presentes nesse destino.

   Por exemplo, se o nome da tarefa de backup for *Demo* e o destino de backup for xxx.xxx.xxx.xxx:/Dados, navegue até o destino de backup e verifique se um novo ponto de recuperação é gerado.

   Os dados de backup são verificados com êxito.

   A tarefa de backup é modificada com êxito e executada novamente.

Como executar uma recuperação em nível de arquivo nos nós do Linux

Uma recuperação em nível de arquivo restaura os arquivos e as pastas individuais a partir de um ponto de recuperação. É possível restaurar um mínimo de um arquivo a partir do ponto de recuperação. Essa opção é útil se você deseja restaurar os arquivos selecionados e não todo o ponto de recuperação.

Execute essas tarefas para uma recuperação em nível de arquivo:

- Verificar os pré-requisitos da restauração
- Especificar o ponto de recuperação para o backup sem agente com base em host
- Especifique o ponto de recuperação para o backup com base em agente
- Especificar os detalhes da máquina de destino
- Especificar as configurações avançadas
  - (Opcional) Gerenciar scripts anteriores e posteriores para automação
- Criar e executar a tarefa de restauração
- Verificar se os arquivos foram restaurados

Verificar os pré-requisitos

Considere as seguintes opções antes de executar uma recuperação em nível de arquivo:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver.
- Você tem um nó de destino válido para recuperar os dados.
- Quando o destino de backup de uma tarefa de backup é o local de origem, para executar uma tarefa de restauração no nível do arquivo do destino é necessário exportar do destino do local de origem por meio de NFS ou CIFS e especificar o ponto de recuperação como disponível no compartilhamento NFS ou CIFS.
- Você verificou se o servidor de backup do Linux oferece suporte ao sistema de arquivos que deseja restaurar.

  Por exemplo, o RedHat 7.x não oferece suporte para o sistema de arquivos *reiserfs.* Se o sistema operacional do servidor de backup for RedHat 7.x e você desejar restaurar o sistema de arquivos reiserfs, instale o driver do sistema de arquivos para oferecer suporte ao reiserfs. Também é possível usar o Live CD do Agente do Arcserve UDP (Linux) para executar a restauração em nível de arquivo já que o Live CD oferece suporte a todos os tipos de sistema de arquivos.
- Você instalou os seguintes pacotes de software no servidor de backup Linux:
  - mdadm
  - kpartx
  - lvm2
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Especificar o ponto de recuperação para o backup sem agente com base em host

Cada vez que você executar um backup com êxito, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no **Assistente de restauração** de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   - A partir do Arcserve UDP:

   a. Clique na guia **Recursos**.

   b. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   c. No painel central, selecione o nó do e clique em **Ações**.

   d. Clique em **Restaurar arquivo** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve UDP (Linux) é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   e. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   - A partir do Agente do Arcserve UDP (Linux):

   a. Abra a interface da web do Agente do Arcserve UDP (Linux).

      Observação: durante a instalação do Agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor. Efetue logon no Agente do Arcserve UDP (Linux).

   b. Clique em **Restaurar** no menu **Assistente** e selecione **Restaurar arquivo**.

      O **Assistente de restauração - restauração de arquivo** é exibido.

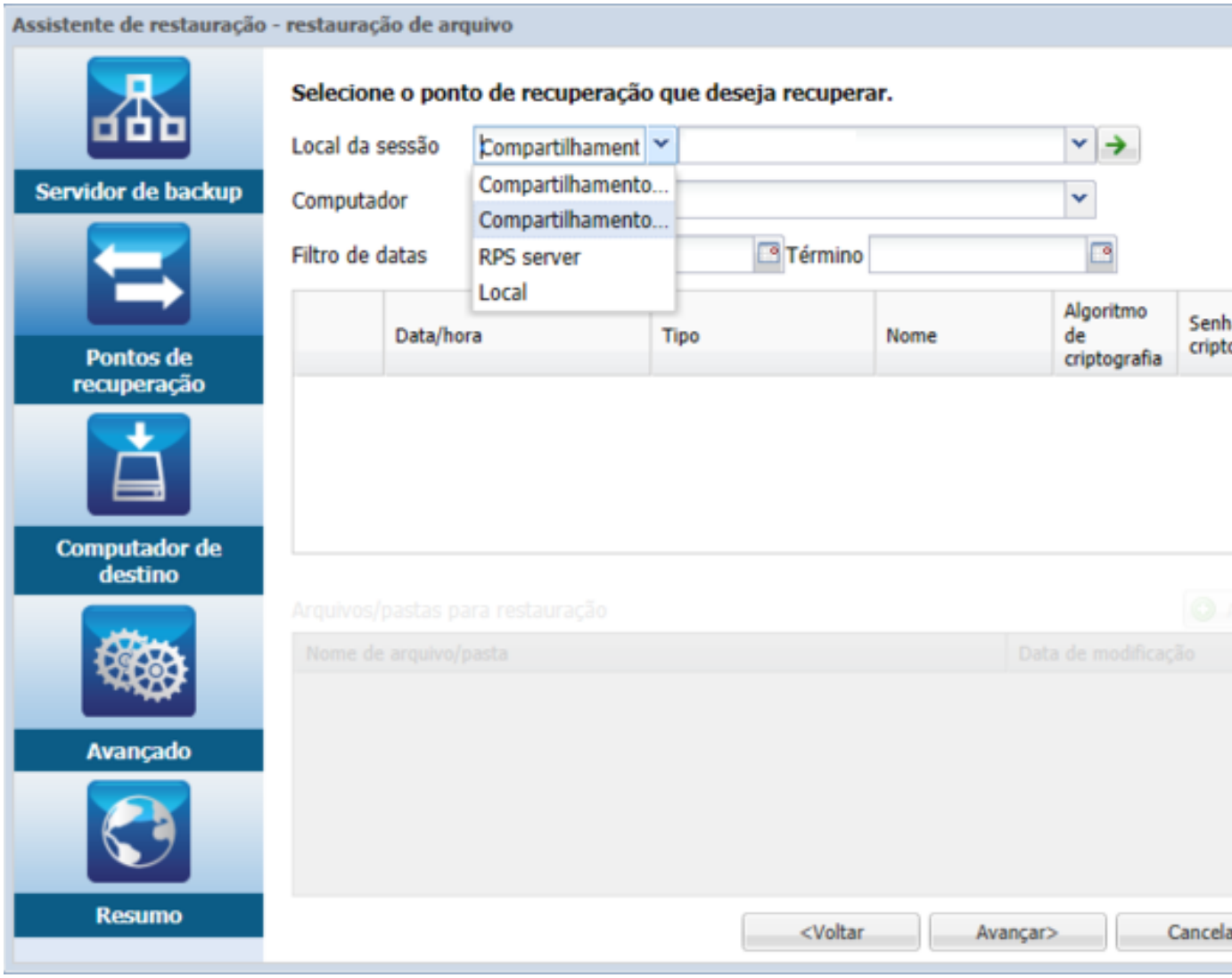
      É possível ver o servidor de backup na página **Servidor de backup** do **Assistente de restauração**.

Não é possível selecionar nenhuma opção na lista suspensa **Servidor de backup**.

2. Clique em **Avançar**.

   A página **Pontos de recuperação** do **Assistente de restauração** é exibida.

   Importante: Se você abrir o Assistente a partir do Console, as informações sobre a máquina e o local da sessão são exibidas automaticamente. Pule para a Etapa 5.



3. Selecione um **Compartilhamento CIFS** ou um **Servidor RPS** na lista suspensa **Local da sessão**.

   Observação: é possível selecionar Local ou compartilhamento de NFS para a restauração de sessões de backup sem agente com base em host.

4. Siga uma das seguintes etapas, dependendo do local da sessão:

   Para o compartilhamento CIFS

   a. Especifique o caminho completo do compartilhamento CIFS e clique em **Conectar**.

   b. Especifique o nome de usuário e a senha para se conectar ao compartilhamento CIFS e clique em **OK**.

   Para o servidor RPS

   a. Selecione o servidor RPS e clique em Adicionar.

      A caixa de diálogo Informações do **servidor de ponto de recuperação** abre.

   a. Forneça os detalhes do RPS e clique em Carregar

   b. Selecione o repositório de dados na lista suspensa e clique em **Sim**.

      A caixa de diálogo **Informações do servidor de ponto de recuperação** fecha e você vê o assistente.

   c. Clique em **Conectar**.

      Todas as máquinas são listadas na lista suspensa Computador.

   d. Selecione o computador na lista suspensa.

      Todos os pontos de recuperação do computador selecionado são exibidos abaixo da opção **Filtro de data**.

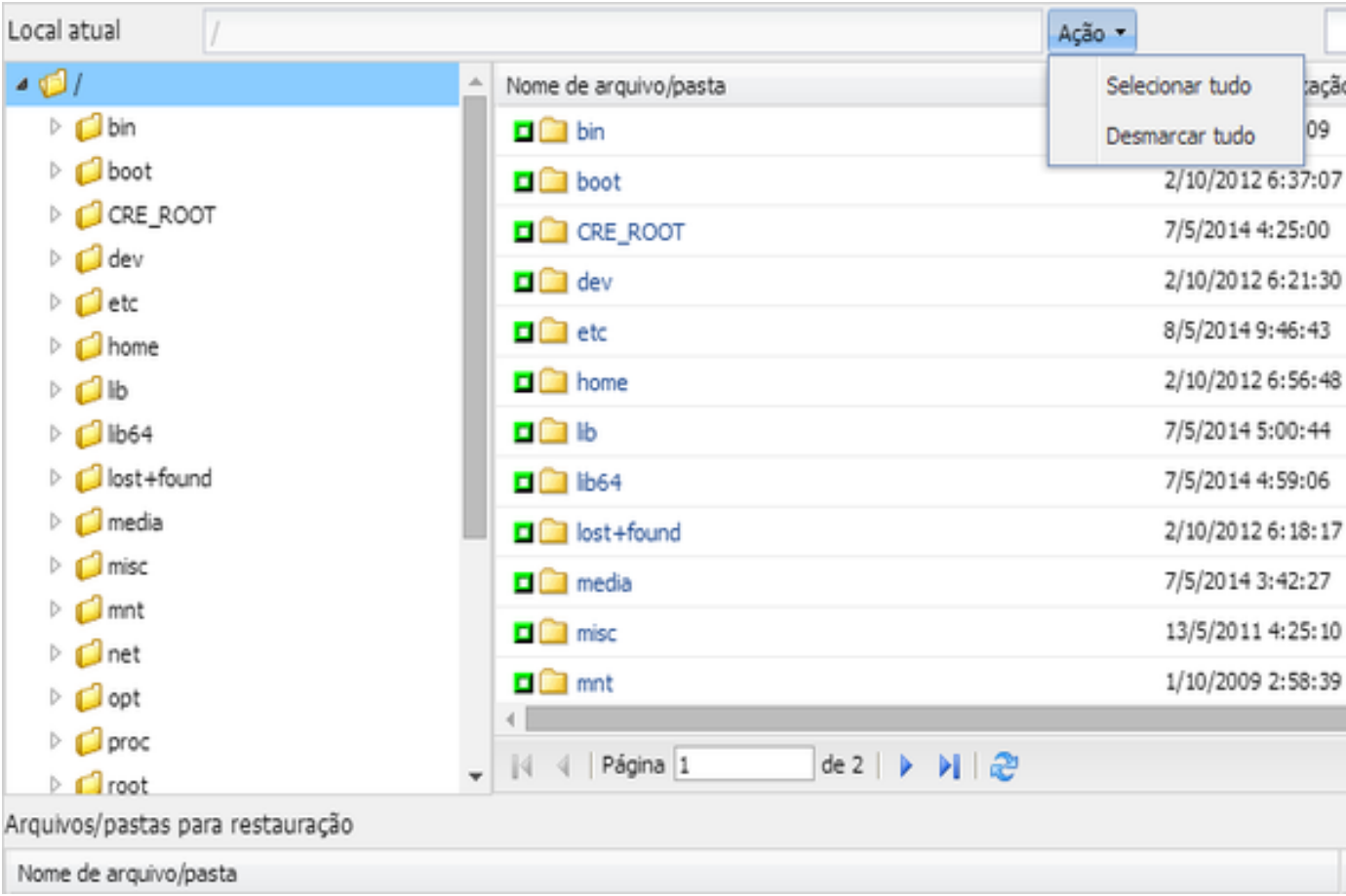
5. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

   Padrão: últimas duas semanas.

   Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

6. Selecione o ponto de recuperação que deseja restaurar e clique em **Adicionar**. Se o ponto de recuperação estiver criptografado, insira a senha de criptografia para restaurar os dados.

   A caixa de diálogo **Procurar-<nome do nó>** é aberta.



Importante: caso você encontre a mensagem de aviso, "os arquivos/pastas são exibidos no arquivo do dispositivo. Clique em Ajuda para obter mais informações." no console, consulte a seguinte Observação para obter uma resolução.

Observação: para alguns layouts de disco complexos, o sistema de arquivos é exibido pelo arquivo do dispositivo. A alteração no comportamento de exibição do sistema de arquivos não afeta a função de restauração de nível de arquivo da VM Linux com base em host. É possível procurar o sistema de arquivos sob o arquivo do dispositivo. Além disso, é possível usar a função de pesquisa para procurar um arquivo ou diretório específico.

7. Selecione os arquivos e as pastas que deseja restaurar e clique em **OK**.

   Observação: se você tentar localizar um arquivo ou pasta usando o campo **Pesquisar**, certifique-se de que tenha selecionado a pasta de nível mais alto na hierarquia. A pesquisa é conduzida em todas as pastas filhas da pasta selecionada.

   A caixa de diálogo **Procurar-<nome de nó>** é fechada e você retorna à página **Pontos de recuperação.** Os arquivos e pastas selecionados são listados em **Arquivos/pastas para restauração**.

8. Clique em **Avançar**.

   A página **Computador de destino** é exibida.

   O ponto de recuperação é especificado.

Especifique o ponto de recuperação para o backup com base em agente

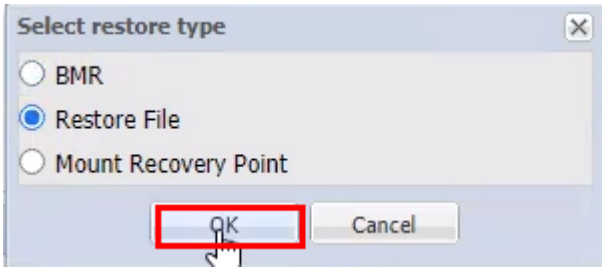
Sempre que você executa um backup, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no Assistente de restauração de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:
   - **A partir do Arcserve UDP :**
     a. Efetue logon no Arcserve UDP.
     b. Navegue até **recursos** > **Nó** > **Todos os nós**.

        Todos os nós adicionados são exibidos no painel central.
     c. Clique com o botão direito do mouse no nó e clique em **Restaurar**.

        A interface da web do agente do Arcserve UDP (Linux) é aberta e exibirá a caixa de diálogo Selecionar o tipo de restauração.
     d. Na caixa de diálogo Selecionar o tipo de restauração, clique na opção **Restaurar arquivo** e clique em **OK**.

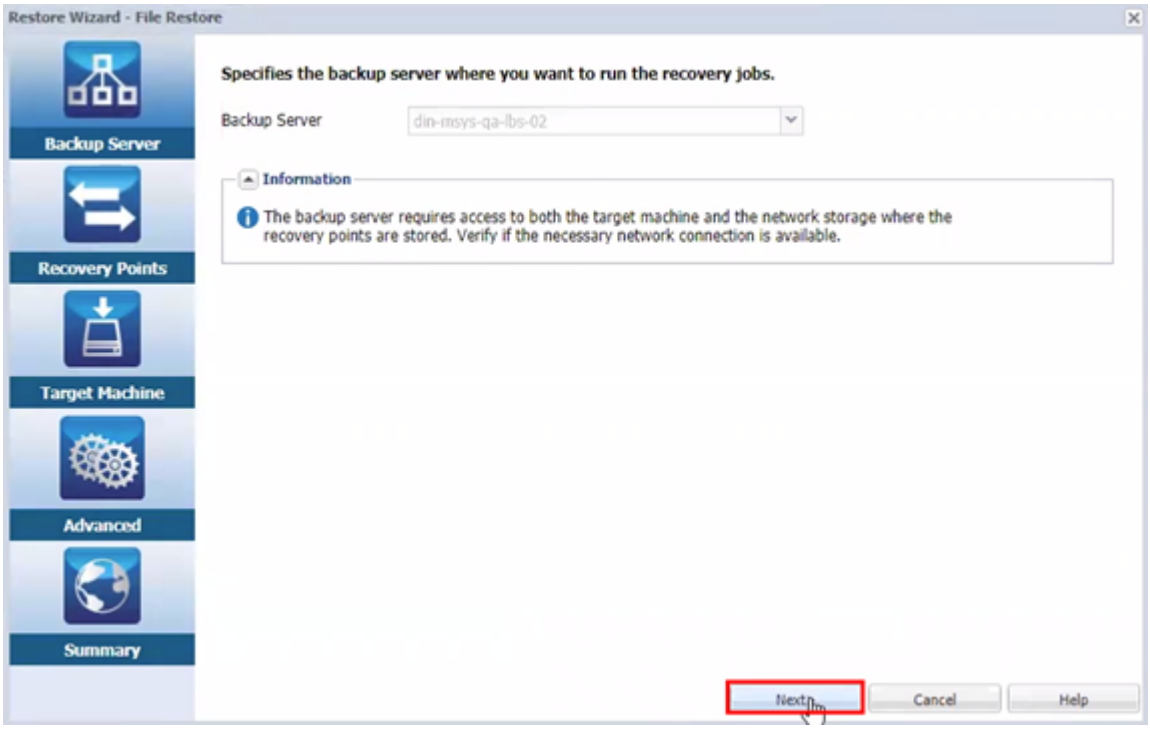
        Observação: você será automaticamente conectado ao nó do agente e o Assistente de restauração será exibido do nó do agente.
   - **A partir do Agente do Arcserve UDP (Linux):**
     a. Abra a interface da web do Agente do Arcserve UDP (Linux).

        Observação: durante a instalação do Agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor. Efetue logon no Agente do Arcserve UDP (Linux).

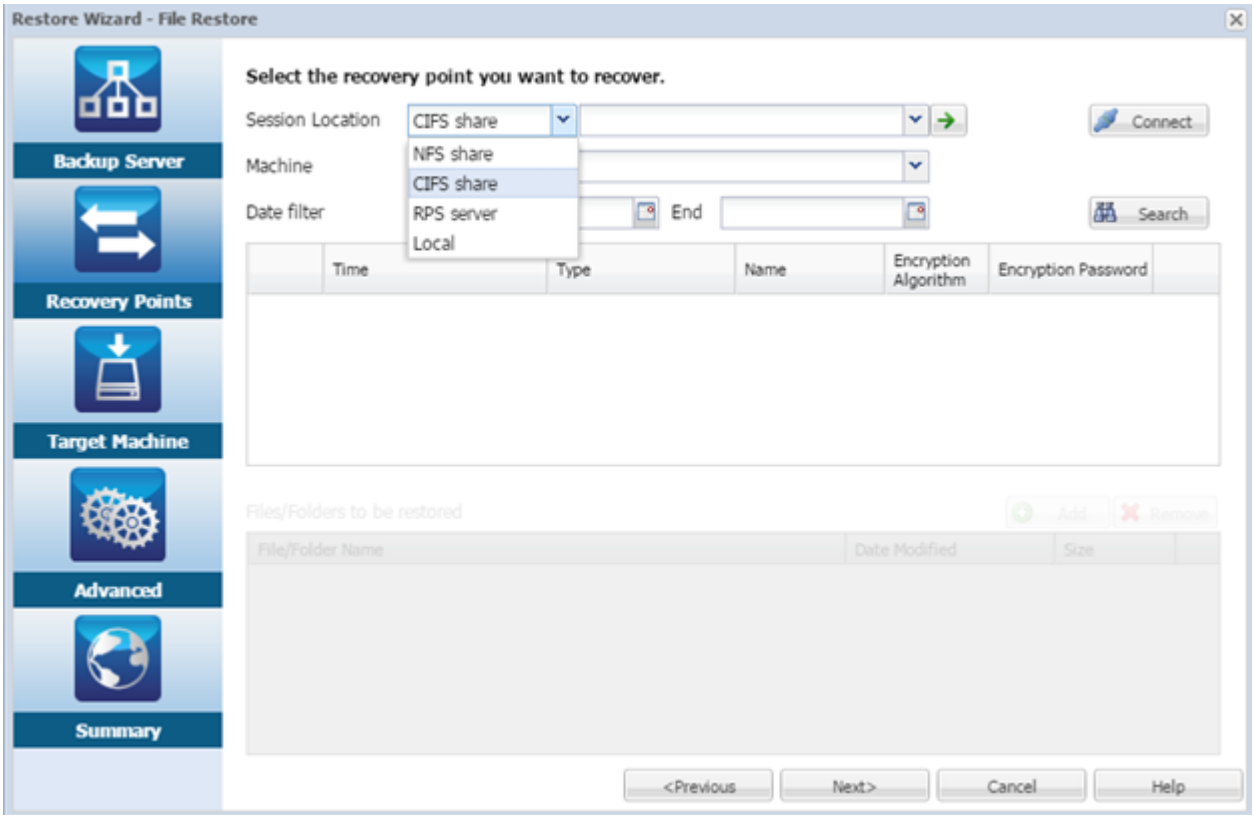
b. No menu Assistente, clique em **Restaurar** e selecione **Restaurar arquivo**.

   A caixa de diálogo Assistente de restauração - Restauração de arquivo é aberta.

2. Na página Servidor de backup do Assistente de restauração, é possível ver o servidor de backup. Não é possível selecionar nenhuma opção na lista suspensa Servidor de backup. Clique em **Avançar**.



3. Na página Pontos de recuperação do Assistente de restauração, faça o seguinte:



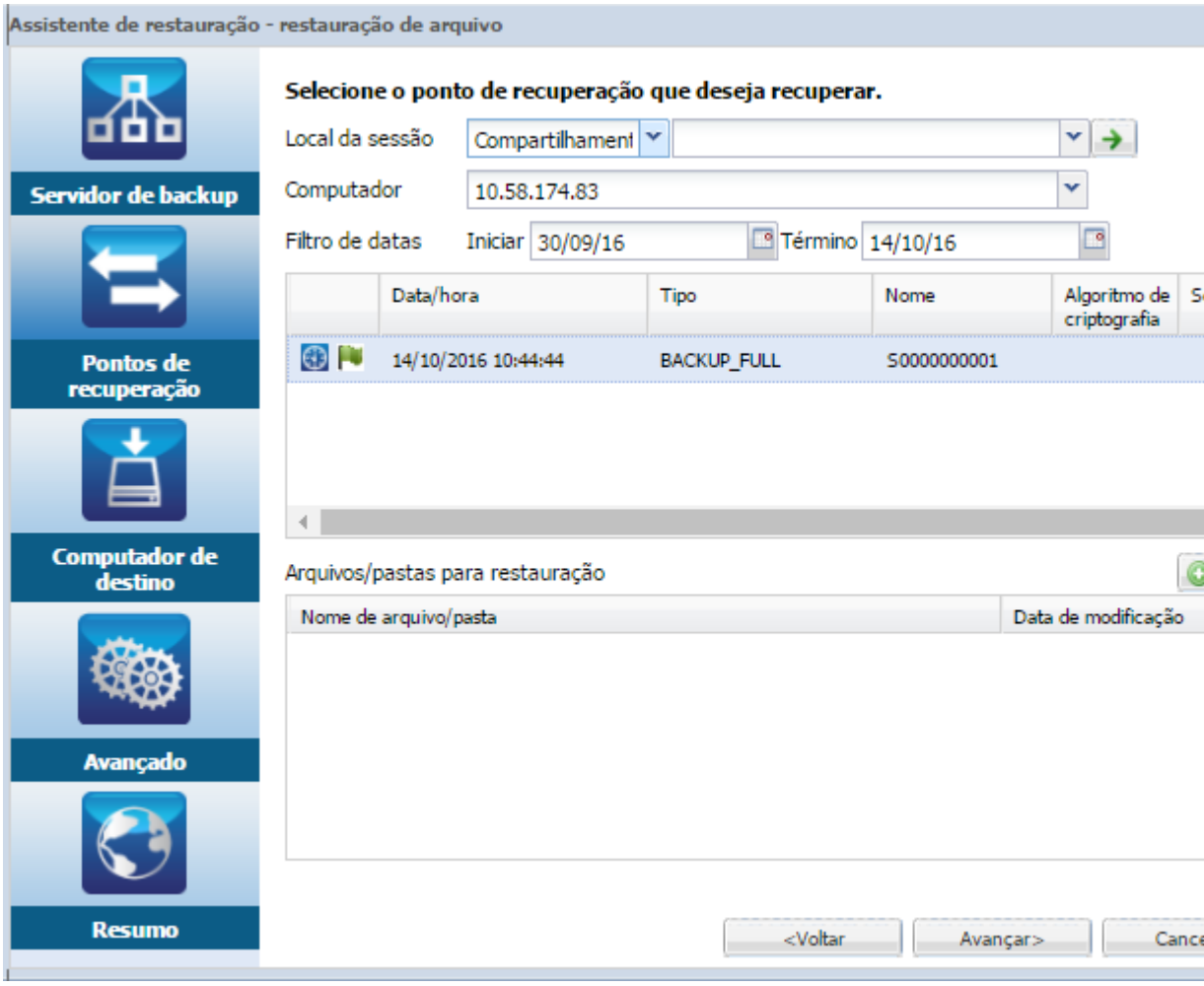
Importante: Se você abrir o Assistente a partir do Console, as informações sobre a máquina e o local da sessão são exibidas automaticamente. Pule para a Etapa 4.

a. Selecione um **compartilhamento CIFS/compartilhamento NFS/servidor RPS/local** na lista suspensa Local da sessão.

b. Se você selecionar o **compartilhamento CIFS/compartilhamento NFS/local**, especifique o caminho completo do compartilhamento CIFS/compartilhamento NFS/local e clique em **Conectar**.

   Todas as máquinas são listadas na lista suspensa Computador.

   Observação: se você selecionar a opção **Compartilhamento CIFS**, especifique o nome de usuário e a senha.



c. Se você selecionar o **servidor RPS**, faça o seguinte:

   1. Selecione o servidor RPS na lista suspensa e clique em **Adicionar**.

      A caixa de diálogo Informações do servidor de ponto de recuperação abre.

   2. Forneça os detalhes do RPS e clique em **Sim**.

   3. Selecione o repositório de dados na lista suspensa.

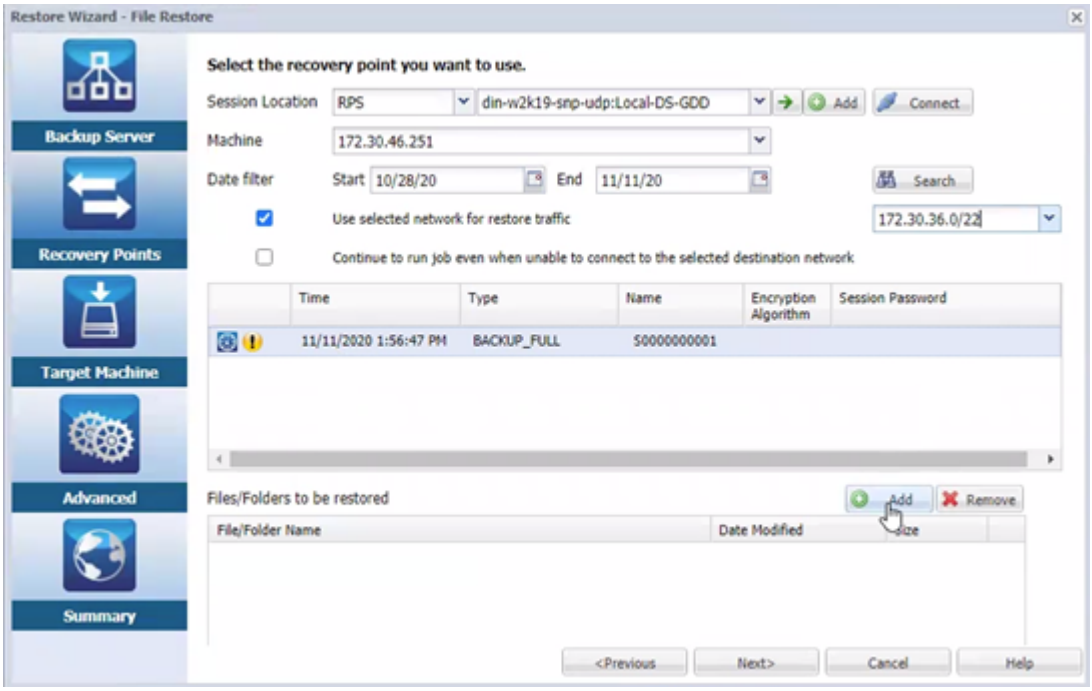
      A caixa de diálogo Informações do servidor de ponto de recuperação fecha e você vê o assistente.

   4. Clique em **Conectar**.

      Todos os nós que foram copiados para backup nesse local são listados na lista suspensa Computador.

   5. Na lista suspensa Computador, selecione o nó que você deseja restaurar.

Todos os pontos de recuperação do nó selecionado são listados.



4. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

   Padrão: últimas duas semanas.

   Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

5. Para ativar a comunicação entre o agente do Linux e o servidor de ponto de recuperação, marque a caixa de seleção **Usar a rede selecionada para restaurar o tráfego** e selecione a rede na lista suspensa.

   Observação: se a rede de backup selecionada não estiver acessível e, para continuar a tarefa de backup com a rede disponível ou com a rede padrão, clique na caixa de seleção **Continuar executando a tarefa mesmo quando não for possível se conectar à rede de backup selecionada**.

6. Selecione o ponto de recuperação que deseja restaurar. Se o ponto de recuperação estiver criptografado, insira a senha de criptografia para restaurar os dados.

7. Para que os arquivos ou as pastas sejam restaurados, clique em **Adicionar**.

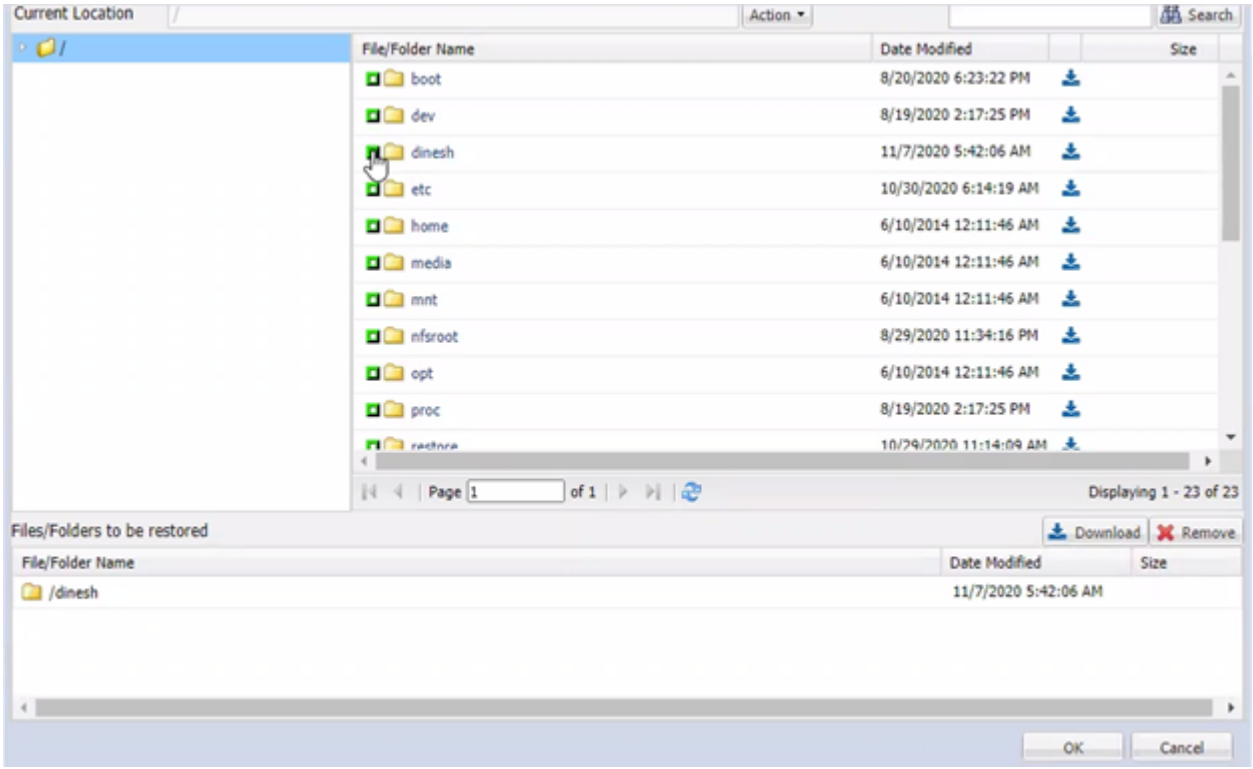
   A caixa de diálogo Procurar-<nome do nó> é aberta.

   Importante: caso você encontre a mensagem de aviso, "os arquivos/pastas são exibidos no arquivo do dispositivo. Clique em Ajuda para obter mais infor-

mações." no console, consulte a seguinte Observação para obter uma resolução.

Observação: para alguns layouts de disco complexos, o sistema de arquivos é exibido pelo arquivo do dispositivo. A alteração no comportamento de exibição do sistema de arquivos não afeta a função de restauração de nível de arquivo da VM Linux com base em host. É possível procurar o sistema de arquivos sob o arquivo do dispositivo. Além disso, é possível usar a função de pesquisa para procurar um arquivo ou diretório específico.

8. Na caixa de diálogo Procurar-<nome do nó>, selecione o arquivo ou a pasta que deseja restaurar e clique em **OK**.



Observação: se você tentar localizar um arquivo ou pasta usando o campo **Pesquisar**, certifique-se de que tenha selecionado a pasta de nível mais alto na hierarquia. A pesquisa é conduzida em todas as pastas filhas da pasta selecionada.

A caixa de diálogo Procurar-<nome de nó> é fechada e você retorna à página Pontos de recuperação. Os arquivos e pastas selecionados são listados em Arquivos/pastas para restauração.

9. Clique em **Avançar**.

   A página Computador de destino é exibida.

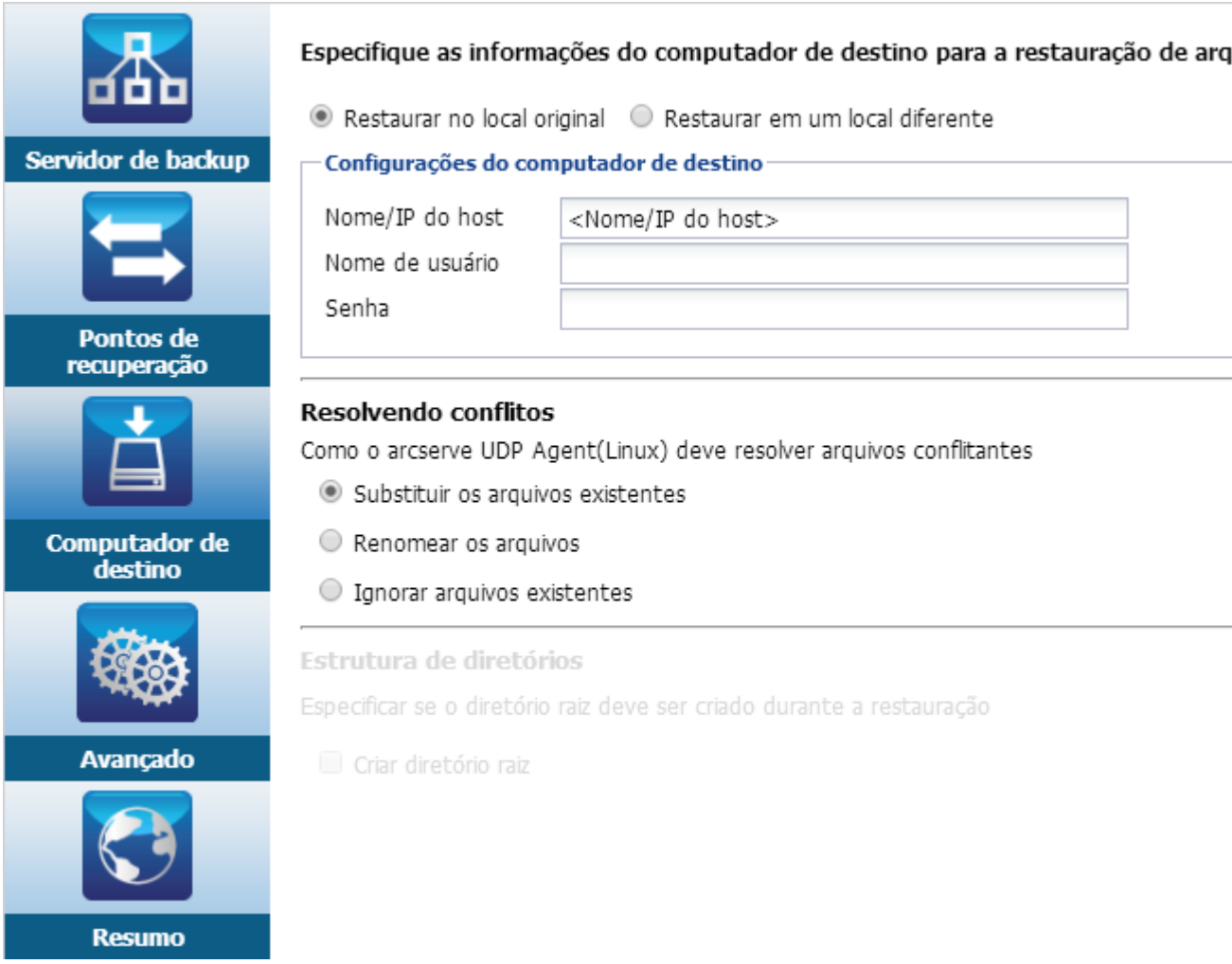
O ponto de recuperação é especificado.

Especificar os detalhes da máquina de destino

Especifique os detalhes do nó de destino, de modo que os dados sejam restaurados para esse nó. É possível restaurar os arquivos ou pastas selecionados no nó de origem ou para um novo nó.

Para fazer a restauração para o nó a partir do qual o backup dos dados foi realizado, siga estas etapas:

1. Na página Computador de destino, selecione **Restaurar ao local original**.



2. Digite o nome de usuário e a senha do nó.
3. Selecione uma das seguintes opções para resolver arquivos conflitantes:

   Substituir arquivos existentes

   Especifica que, se o arquivo existe no computador de destino, o arquivo de backup do ponto de recuperação substituirá o arquivo existente.

   Renomear arquivos

Especifica que, se o arquivo existir no computador de destino, será criado um novo arquivo com o mesmo nome de arquivo e extensão de arquivo *.d2dduplicate<x>*. <x> especifica o número de vezes que o arquivo é restaurado. Todos os dados serão restaurados para o novo arquivo.

Ignorar arquivos existentes

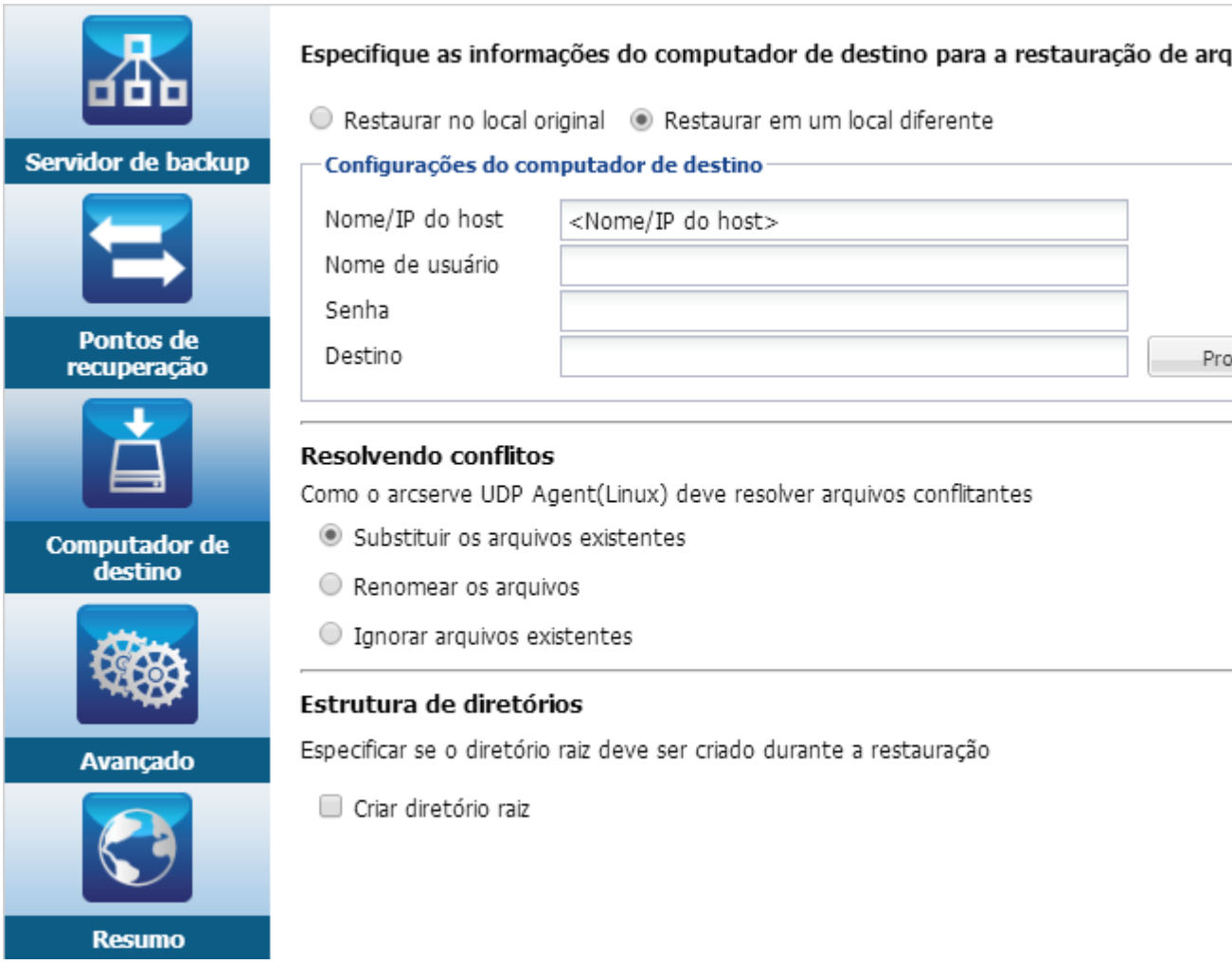
Especifica que, se o mesmo arquivo existe no computador de destino, esses arquivos não serão restaurados a partir do ponto de recuperação.

4. (Opcional) Selecione **Criar diretório raiz**.
5. Clique em **Avançar**.

   A página Avançado é exibida.

Para restaurar em um novo nó, siga estas etapas:

1. Na página Computador de destino, selecione **Restaurar ao local alternativo**.



2. Digite o nome do host ou o endereço IP do nó de destino.

3. Digite o nome de usuário e a senha do nó.
4. Digite o caminho onde os dados são restaurados ou clique em **Procurar** para selecionar a pasta na qual os dados serão restaurados e clique em **OK**.
5. Selecione uma das seguintes opções para resolver arquivos conflitantes:

   Substituir arquivos existentes

   Especifica que, se o arquivo existe no computador de destino, o arquivo de backup do ponto de recuperação substituirá o arquivo existente.

   Renomear arquivos

   Especifica que, se o arquivo existir no computador de destino, será criado um novo arquivo com o mesmo nome de arquivo e extensão de arquivo *.d2dduplicate<x>*. <x> especifica o número de vezes que o arquivo é restaurado. Todos os dados serão restaurados para o novo arquivo.

   Ignorar arquivos existentes

   Especifica que, se o mesmo arquivo existe no computador de destino, esses arquivos não serão restaurados a partir do ponto de recuperação.
6. (Opcional) Selecione **Criar diretório raiz**.
7. Clique em **Avançar**.

   A página Avançado é exibida.

Os detalhes do computador de destino são especificados.

Especificar as configurações avançadas

Especifique as configurações avançadas para executar uma recuperação programada de seus dados. A recuperação programada assegura que os dados sejam recuperados no horário especificado, mesmo em sua ausência.

Siga estas etapas:

1. Defina a hora e data de início, selecionando uma das seguintes opções:

   Executar agora

   Inicia a tarefa de restauração em nível de arquivo assim que você enviar a tarefa.

   Definir data e hora de início

   Inicia a tarefa de restauração em nível de arquivo na data e hora especificadas, após enviar a tarefa.

2. (Opcional) Selecione **Estimativa de tamanho do arquivo**.
3. (Opcional) Selecione um script a partir da opção **Configurações de scripts anteriores e posteriores**.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos Configurações de scripts anteriores e posteriores serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local:

   `/opt/Arcserve/d2dserver/usr/prepost`

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.

4. Clique em **Avançar**.

   A página **Resumo** é exibida.

   As configurações avançadas são especificadas.

(Opcional) Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar os scripts em **Configurações de scripts anteriores e posteriores** do **Assistente de backup** e do **Assistente de restauração** na interface do usuário. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

Variáveis de ambiente de script anterior e posterior

Para criar seu script, use as seguintes variáveis de ambiente:

D2D_JOBNAME

Identifica o nome da tarefa.

D2D_JOBID

Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

D2D_TARGETNODE

Identifica o nó cujo backup está sendo feito ou restaurado.

D2D_JOBTYPE

Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

backup.full

Identifica a tarefa como um backup completo.

backup.incremental

Identifica a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino antes do início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

/opt/Arcserve/d2dserver/usr/prepost

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   `/opt/Arcserve/d2dserver/usr/prepost`

2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.
6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de

backup especificada.

O script é executado.

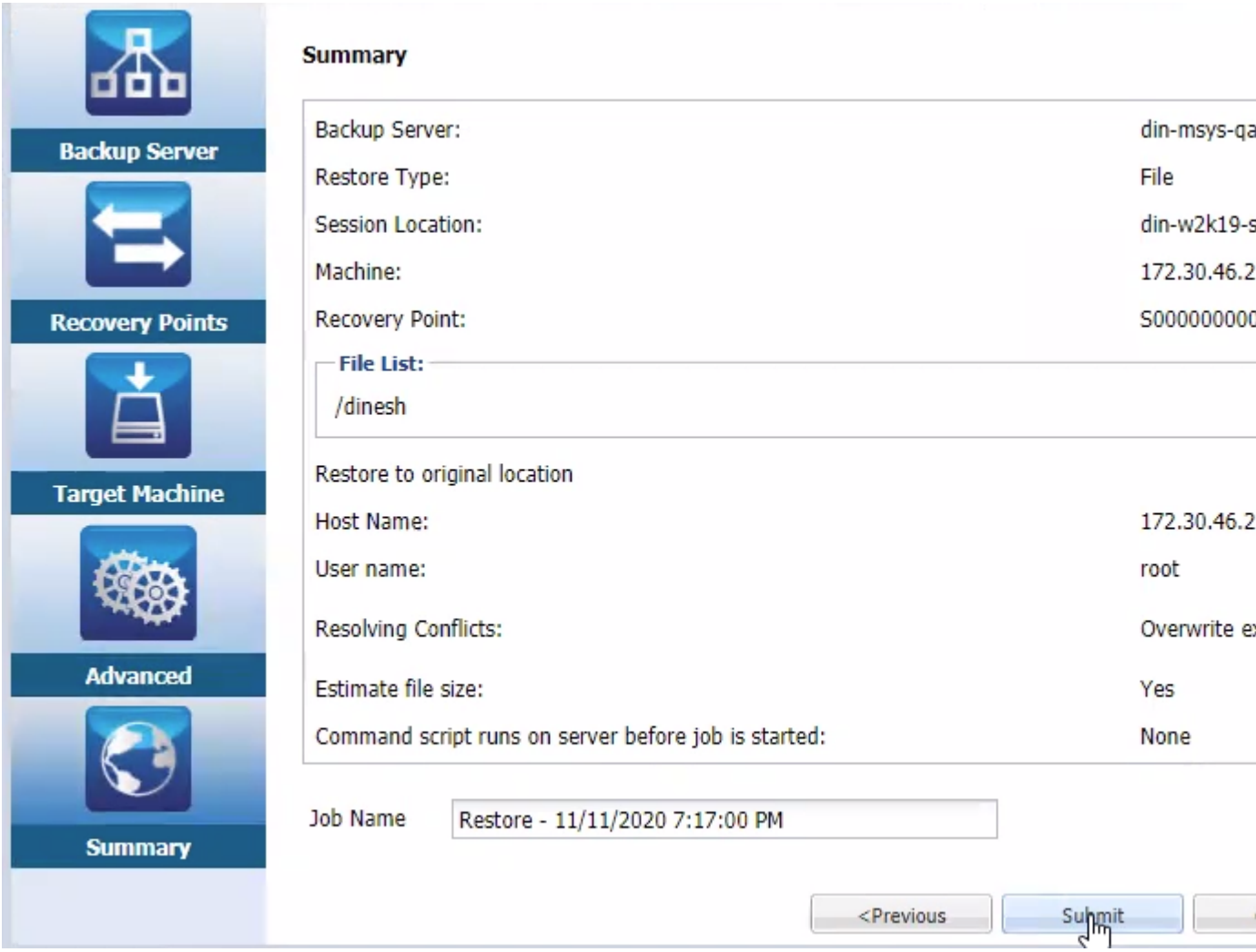
Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Criar e executar a tarefa de restauração

Crie e execute a tarefa de restauração, para poder iniciar a recuperação de nível de arquivo. Verifique as informações do ponto de recuperação antes de restaurar os arquivos. Se necessário, volte e altere as configurações de restauração no assistente.

Siga estas etapas:

1. Na página Resumo do Assistente de restauração, verifique os detalhes da restauração.



2. Siga um destes procedimentos:
   - Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, digite um nome de tarefa e clique em **Enviar** para iniciar o processo de restauração.

Observação: o campo Nome da tarefa tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

O Assistente de restauração é fechado. É possível ver o status da tarefa na guia Status da tarefa.

A tarefa de restauração é criada e executada com êxito.

Verificar se os arquivos foram restaurados

Após a conclusão da tarefa de restauração, certifique-se de que todos os arquivos estejam restaurados no nó de destino. Verifique as guias **Histórico da tarefa** e **Log de atividades** no painel **Status** para monitorar o andamento do processo de restauração.

Siga estas etapas:

1. Navegue para o computador de destino em que você restaurou os dados.
2. Verifique se os dados necessários do ponto de recuperação foram restaurados.

   Os arquivos são verificados com êxito.

   A recuperação em nível de arquivo é executada com êxito.

Como criar um Live CD inicializável

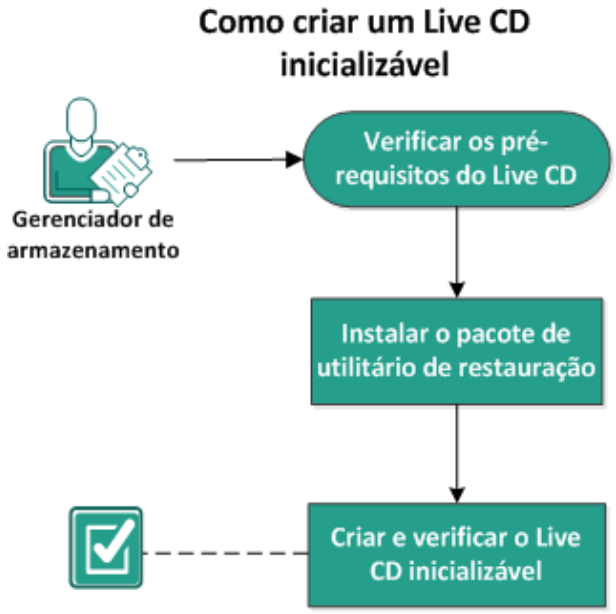
Como um gerenciador de armazenamento, é possível criar um Live CD inicializável. Quando criado, esse Live CD inicializável contém uma imagem somente leitura completa do sistema operacional do computador, e pode ser usado para fornecer a funcionalidade do sistema operacional temporário. Esse Live CD inclui todas as configurações do sistema e arquivos do sistema operacional, e pode ser usado para executar as seguintes funções:

- É possível usar o Agente do Arcserve UDP (Linux) sem instalar de fato o produto. Isso permite que você experimente e avalie o produto sem instalá-lo nem fazer alterações no disco rígido do seu computador.
- É possível instalar o Agente do Arcserve UDP (Linux) (em vários servidores) usando apenas um pacote de configuração. Sem um Live CD, é preciso instalar dois arquivos separados (arquivo .bin e pacote do utilitário de restauração) para instalar o Agente do Arcserve UDP (Linux). O pacote do utilitário de restauração está incluído no mesmo pacote de instalação do Live CD.
- É possível executar uma BMR (Bare Metal Recovery - Recuperação Bare-Metal). É possível usar o Live CD para obter o endereço IP da máquina de destino (que é necessário durante a BMR).

A pasta bin contém os scripts que podem ser executados na linha de comando para criar um Live CD inicializável. A pasta bin está localizada no seguinte caminho:

```
# /opt/Arcserve/d2dserver/bin
```

O diagrama a seguir exibe o processo para criar um Live CD inicializável:



A lista a seguir descreve as tarefas para criar um Live CD inicializável:

- Verificar os pré-requisitos do Live CD
- Instalar o pacote de utilitário de restauração
- Criar e verificar o Live CD inicializável

Verificar os pré-requisitos do Live CD

Considere os seguintes pré-requisitos antes de criar um Live CD:

- Você tem as credenciais de logon raiz para efetuar logon no servidor de backup.
- Você precisa ler as Notas da Versão para entender as funções de um Live CD.
- Deve ter o conhecimento de execução de scripts Linux.
- Você instalou a ferramenta *mkisofs* no servidor do backup. O servidor de backup usa a ferramenta mkisofs para criar o arquivo Live CD.iso.
- Você tem pelo menos de 1024 MB de memória livre no computador para inicializar e executar o Live CD.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Instalar o pacote de utilitário de restauração

Você deve instalar o pacote de utilitário de restauração para executar as operações de restauração. Se você não instalar o pacote de utilitário de restauração, não será possível executar a restauração em nível de arquivos ou a BMR. É possível instalar o pacote de utilitário de restauração durante a instalação do Agente do Arcserve UDP (Linux). Também é possível fazer download do pacote de utilitário de restauração e instalá-lo a qualquer momento após a instalação do Agente do Arcserve UDP (Linux).

Após instalar o pacote de utilitário de restauração, é possível criar um Live CD.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Navegue para a pasta bin usando o seguinte comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

3. Execute o comando a seguir para instalar o pacote de utilitário de restauração:

   ```
   #./configutility
   ```

   Uma mensagem é exibida solicitando que você forneça o caminho do pacote do utilitário de restauração.

4. Forneça o caminho completo onde você fez download do pacote do utilitário de restauração.

   A instalação é iniciada.

   O pacote de utilitário de restauração é instalado.

Criar e verificar o Live CD inicializável

O Live CD cria o ambiente do servidor de backup sem instalar o software. O Live CD facilita a BMR usando o IP em uma rede privada.

Live CD é um sistema operacional de computador inicializável completo que é executado na memória do computador, em vez de ser no carregamento do disco rígido. O Live CD permite que você experimente e avalie um sistema operacional sem instalá-lo nem alterar o sistema operacional existente no computador.

Siga estas etapas:

1. Navegue para a pasta bin usando o seguinte comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

2. Execute o seguinte comando para criar um Live CD:

   ```
   # ./makelivecd
   ```

3. Vá até o seguinte local e verifique se o arquivo LiveCD.iso foi criado:

   ```
   /opt/Arcserve/d2dserver/packages
   ```

   Você criou e verificou com êxito o Live CD inicializável. Se desejar usar o Live CD em uma rede virtual, é possível montar o arquivo LiveCD.iso diretamente na máquina virtual. Se desejar usar o Live CD em um computador físico, será preciso gravar a imagem do LiveCD.iso em um arquivo de mídia (CD ou DVD) e, em seguida, usar o arquivo de mídia para inicializar o computador.

Como usar o Live CD como um servidor de backup do Linux

É possível usar o live CD como um servidor de backup Linux.

Siga estas etapas:

1. Crie um Live CD no servidor de backup Linux.

   Para criar o Live CD, na página inicial:

   - Clique em Restaurar, BMR (Bare Metal Recovery - Recuperação Bare Metal)
   - A partir do Assistente de restauração - BMR, clique no link **Clique aqui para fazer download do Live CD** e salvar como o Live CD.

2. Inicie uma máquina virtual ou física com o Live CD.

   Observação: recomendamos 4 GB de memória para este computador.

   Quando o computador for iniciado com o Live CD, é possível exibir a seguinte mensagem:

   Use o seguinte URL para acessar e gerenciar esse Agente do Arcserve UDP (Linux): https://xxx.xxx.xxx.xxx:8014.

   xxx.xxx.xxx.xxx refere-se ao URL atual que o computador está usando.

3. Digite o URL *https://xxx.xxx.xxx.xxx:8014* em seu navegador.

   A página inicial do servidor de backup Linux aparece.

4. Use as funções do servidor de backup Linux para executar uma tarefa.

   Por exemplo: clique em Restauração, Restaurar arquivo, localize o local da sessão de backup e execute a tarefa de restauração em nível de arquivo.

Como criar um Live CD com base em CentOS

Importante:

- No momento, o ISO do CentOS8.0 LiveGNOME não está disponível no site do CentOS. Portanto, para o UDP 8.0, não oferecemos suporte à criação de um LiveCD inicializável para o CentOS 8 para incluir drivers personalizados. Caso ainda queira incluir drivers personalizados específicos ao LiveCD, use o CentOS 7 com UDP 8.0 para o sistema operacional recomendado da release 8.0.
- Se não houver uma necessidade específica de incluir drivers personalizados, use o LiveCD padrão (UDP_Agent_Linux-LiveCD.iso), que está disponível na versão 8.0 do LBS para executar a BMR em um nó de destino.

Como gerenciador de armazenamento, é possível criar um Live CD inicializável com base em CentOS. O Live CD CentOS é um ambiente de computação em memória com base em CentOS. A finalidade deste Live CD é fornecer aos usuários a capacidade de usar a funcionalidade CentOS sem instalar o CentOS. O Live CD é executado na memória sem que haja impacto no disco rígido. As alterações que você fizer no ambiente de tempo de execução do Live CD são perdidas após a reinicialização do computador.

Esse Live CD inclui todas as configurações do sistema e arquivos do sistema operacional, e pode ser usado para executar as seguintes funções:

- É possível usar o Agente do Arcserve UDP (Linux) sem instalar de fato o produto. Isso permite que você experimente e avalie o produto sem instalá-lo nem fazer alterações no disco rígido do seu computador.
- É possível executar uma BMR (Bare Metal Recovery - Recuperação Bare-Metal). É possível usar o Live CD para obter o endereço IP da máquina de destino (que é necessário durante a BMR).

Quando usar o Live CD com base em CentOS:

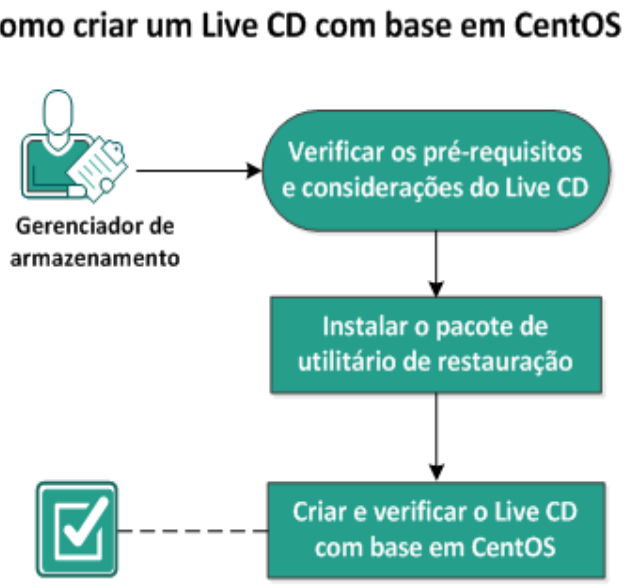
Quando o Live CD padrão não puder identificar o dispositivo de armazenamento e o dispositivo de rede devido à falta do driver de dispositivo.

Observação: os pontos de recuperação que deseja restaurar não incluem os drivers de dispositivo do sistema de armazenamento do computador de BMR de destino. Como resultado, o Agente do Arcserve UDP (Linux) bloqueará qualquer tentativa de executar uma tarefa de BMR em um estágio inicial.

A pasta bin contém os scripts que podem ser executados na linha de comando para criar um Live CD inicializável. A pasta bin está localizada no seguinte caminho:

```
# /opt/Arcserve/d2dserver/bin
```

O diagrama a seguir exibe o processo para criar um Live CD com base em CentOS:



Execute as tarefas a seguir para criar um cenário do Live CD com base em CentOS:

- Verificar os pré-requisitos e considerações do Live CD
- Instalar o pacote de utilitário de restauração
- Criar e verificar o Live CD com base em CentOS

Verificar os pré-requisitos e considerações do Live CD

Antes de criar um Live CD com base em CentOS, examine a seguinte tabela que compara o Live CD padrão com o Live CD do CentOS:

Parâmetros	Live CD padrão	Live CD com base em CentOS
Mídia de instalação do servidor de backup	Compatível	Não compatível
Interface de usuário do desktop	Não compatível. Os usuários devem usar o navegador em um computador com Windows para navegar na interface de usuário da web do servidor de backup.	Compatível. O Live CD com base em CentOS inclui um navegador. Os usuários não precisam de outros navegadores para navegar na interface de usuário da web do servidor de backup.
Tamanho da imagem	Aproximadamente 1,1 GB.	Aproximadamente 1,9 GB.
Driver de dispositivo adicional para o Live CD	Não compatível	Compatível
BMR local **(Recuperar o computador sem instalar outro servidor de backup)**	Compatível	Compatível
Imagem de inicialização do PXE	Compatível	Não compatível
Remover CD/ISO do computador de destino da BMR após a inicialização do computador	Compatível	Não compatível. O DVD/ISO deve estar montado no computador de destino da BMR o tempo todo durante o processo de recuperação, até à conclusão da tarefa de BMR e à reinicialização do computador.
Ambiente do sistema operacional do Live CD em inglês	Sim	Sim. Interface do computador também em inglês
Idioma localizado para a interface do usuário da web do servidor de backup	Sim	Sim

Suporte para o tipo de nó	Suporte para computador físico, servidor VMWare ESX, OVM, Citrix Xen VM	Suporte apenas para computador físico e VM do servidor do VMware ESX

Considere os seguintes pré-requisitos antes de criar um Live CD com base em CentOS:

- Verifique se você instalou os seguintes pacotes de software no servidor de backup:
  - genisoimage
  - squashfs-tools
- O Live CD com base em CentOS pode inicializar somente a partir de um computador físico e VM do servidor ESX. Ele não oferece suporte a outras soluções de virtualização.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Instalar o pacote de utilitário de restauração

Você deve instalar o pacote de utilitário de restauração para executar as operações de restauração. Se você não instalar o pacote de utilitário de restauração, não será possível executar a restauração em nível de arquivos ou a BMR. É possível instalar o pacote de utilitário de restauração durante a instalação do Agente do Arcserve UDP (Linux). Também é possível fazer download do pacote de utilitário de restauração e instalá-lo a qualquer momento após a instalação do Agente do Arcserve UDP (Linux).

Após instalar o pacote de utilitário de restauração, é possível criar um Live CD.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Navegue para a pasta bin usando o seguinte comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

3. Execute o comando a seguir para instalar o pacote de utilitário de restauração:

   ```
   # ./configutility
   ```

   Uma mensagem é exibida solicitando que você forneça o caminho do pacote do utilitário de restauração.

4. Forneça o caminho completo onde você fez download do pacote do utilitário de restauração.

   A instalação é iniciada.

   O pacote de utilitário de restauração é instalado.

Criar e verificar o Live CD com base em CentOS

É possível usar esse Live CD para iniciar o computador de destino da BMR e executar novamente a tarefa de BMR. Os arquivos a seguir são usados para criar o Live CD com base em CentOS:

makelivecd.centos

Um script usado para remasterizar o Live CD do CentOS.

CentOS-7-x86_64-LiveGNOME.ISO

Uma imagem ISO do Live CD do CentOS. A imagem pode ser baixada no site do CentOS.

Importante: Ao criar um Live CD inicializável para CentOS 7, faça download e use a imagem *CentOS-7-x86_64-LiveGNOME.ISO* em vez de CentOS-7-x86_64-LiveCD.ISO no site do sistema operacional Cent.

O ponto de recuperação sendo restaurado não contém o driver de dispositivo referente ao sistema de armazenamento do computador da BMR de destino. O Agente do Arcserve UDP (Linux) bloqueia essa tarefa de BMR em um estágio inicial.

Siga estas etapas:

1. Prepare os drivers de dispositivo (arquivos *.ko e *.rpm) para CentOS e armazene-os em uma pasta.

   Exemplo: armazene os drivers de dispositivo na pasta /tmp/drivers.

   Observação: é necessário fornecer o driver de dispositivo que corresponda à versão do kernel do Live CD do CentOS.

2. Acesse o site do CentOS e faça download do Live CD do CentOS 7.0 de 64 bits ou posterior para a pasta /tmp no servidor de backup.

   O arquivo *CentOS-7-x86_64-LiveGNOME.ISO* é baixado.

3. Navegue até a pasta bin (/opt/Arcserve/d2dserver/bin) e execute o seguinte comando:

   ```
   makelivecd.centos <full_path_to_
   CentOS_live_cd> [path_where_device_
   drivers_are_stored]
   ```

   Exemplo: ./makelivecd.centos <full_path_to_CentOS_live_cd> /tmp/drivers

O script cria o Live CD do Arcserve UDP para Linux com base no CentOS e armazena o arquivo de imagem ISO no seguinte local:

```
/opt/Arserve/d2dserver/packages/
CentOS-LiveCD-for-UDP_
Agent_Linux.iso
```

4. Navegue até a pasta de pacotes e verifique se o arquivo CentOS-LiveCD-for-UDP_Agent_Linux.iso está na pasta.

   O Live CD com base em CentOS é criado e verificado.

   Você criou com êxito um Live CD com base em CentOS.

Como criar um Live CD inicializável para incluir drivers personalizados para o CentOS 8.X

O recurso de Live CD personalizado permite criar um Live CD inicializável para o CentOS 8.0 para incluir os drivers personalizados.

Quando usar o Live CD personalizado:

Use o Live CD personalizado quando o Live CD padrão não conseguir identificar os dispositivos de armazenamento e de rede devido à indisponibilidade de um driver de dispositivo.

Observação: os pontos de recuperação que deseja restaurar não incluem os drivers de dispositivo do sistema de armazenamento do computador de BMR de destino. Como resultado, o agente do Arcserve Unified Data Protection para Linux bloqueará qualquer tentativa de executar uma tarefa de BMR em um estágio inicial.

A pasta bin contém os scripts que podem ser executados na linha de comando para criar um Live CD inicializável. A pasta bin está localizada no seguinte caminho:

 # /opt/Arcserve/d2dserver/bin

Verificar pré-requisitos

Estas tarefas de pré-requisito devem ser concluídas:

1. O UDPLinux 8.1 ou uma versão posterior deve ser instalado no LBS.
2. Os drivers de dispositivo (arquivos *.ko ou *.rpm) devem ser preparados e armazenados em uma pasta dentro do LBS.

   Por exemplo, armazene os drivers de dispositivo na pasta /tmp/drivers.

   Observação: é necessário fornecer o driver de dispositivo que corresponda à versão do kernel do Live CD padrão do UDPLinux. No momento, as versões do sistema operacional e do kernel para o Live CD do UDP Linux são as seguintes:

   - Versão do sistema operacional: Centos 8.0
   - Versão do kernel: 4.18.0-80.el8.x86_64
3. Para criar um Live CD personalizado dentro do LBS, deve haver espaço suficiente alocado.

   Por exemplo, se o caminho desejado para o Live CD personalizado de saída for /tmp/iso, o espaço do local /tmp/iso deverá ser maior ou igual ao tamanho do Live CD padrão mais o tamanho total do(s) driver(s) e rpm(s) do usuário e mais 500 MB.

Criar o Live CD personalizado

O recurso Live CD personalizado permite inicializar um computador de destino da BMR e executar uma tarefa de BMR. Para criar um Live CD personalizado, os seguintes arquivos são usados:

driverinlivecd

Um script usado para remasterizar o Live CD padrão.

UDP_Agent_Linux-LiveCD.iso

Live CD padrão disponível para o agente do UDP para Linux.

Siga estas etapas:

1. Vá até o seguinte local:

   /opt/Arcserve/d2dserver/bin

2. Execute o seguinte comando:

   driverinlivecd <caminho_completo_para_LiveCD_padrão> <caminho_de_armazenamento do(s)_driver(s)_de_dispositivo> <caminho_para_armazenamento_do_LiveCD_personalizado>

   Exemplo:/driverinlivecd /opt/Arcserve/d2dserver/packages/UDP_Agent_Linux-LiveCD.iso /tmp/drivers /tmp/iso

   O script cria o Live CD personalizado com base no(s) driver(s) de dispositivo fornecido(s) e, em seguida, armazena o arquivo de imagem ISO no local desejado.

   Exemplo: */tmp/iso/ UDP_Agent_Linux-LiveCD.iso*

Verificar o Live CD personalizado

Esta seção fornece informações sobre como verificar o Live CD personalizado.

Siga estas etapas:

1. Inicialize um nó de destino com o Live CD personalizado resultante (UDP_ Agent_Linux-LiveCD.iso) criado no local desejado:

   /tmp/iso/

2. Abra o shell ou a linha de comando.
3. Para verificar se os rpms estão incluídos no Live CD personalizado, execute o seguinte comando:

   ls /user_rpms/

4. Para verificar se os arquivos *.ko estão incluídos no Live CD personalizado, execute o seguinte comando:

   ls /lib/modules/4.18.0-80.el8.x86_64/kernel/drivers/users/

5. Verifique as informações dos drivers de dispositivo.

   Exemplo: modinfo "nome_do_driver"

   Se a saída não estiver vazia/NULL, ela deverá mostrar as informações sobre o driver de dispositivo carregado.

   O Live CD personalizado foi verificado com êxito. Agora, você pode executar a tarefa de BMR para o nó de origem desejado.

Observações:

- No caso de pacotes rpm, verifique se os pacotes podem ser instalados usando simplesmente os utilitários rpm e se não deve haver nenhuma outra dependência ou pacotes pendentes.

  Por exemplo, para verificar, tente instalar o pacote rpm na própria VM do CentOS 8.0 (kernel: 4.18.0-80.el8.x86_64), antes de usar o recurso.

- Se os pacotes rpm contiverem drivers de dispositivo (arquivos *.ko), pode acontecer que os drivers às vezes não sejam carregados corretamente no nó de destino após a execução do script *driverinlivecd* e a criação do Live CD personalizado. Caso isso ocorra, extraia os pacotes rpm para obter os arquivos *.ko necessários, que devem ser carregados no nó de destino. Ao executar o script *driverinlivecd*, mantenha os arquivos *.ko exatamente no caminho em que os drivers de dispositivo estão armazenados, em vez de manter o pacote rpm.

Como executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal) para computadores Linux

Uma BMR restaura o sistema operacional e os aplicativos de software e recupera todos os dados incluídos no backup. A BMR é o processo de restauração de um sistema de computador do estado *bare metal*. Bare metal é um computador sem sistema operacional, drivers e aplicativos de software. Depois que a restauração for concluída, o computador de destino será reinicializado automaticamente no mesmo ambiente operacional que o nó de origem do backup e todos os dados serão restaurados. teste

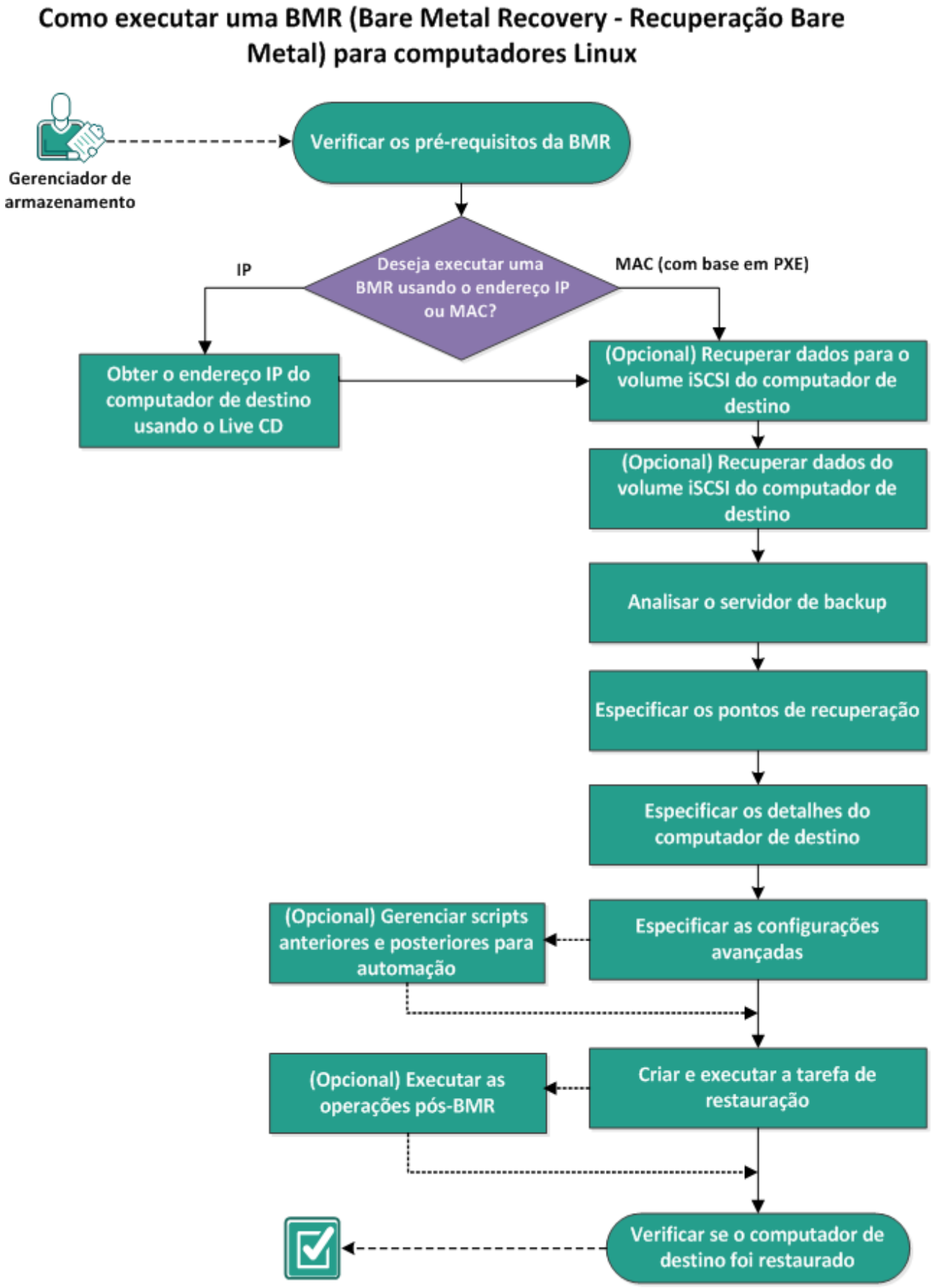
Uma BMR completa é possível porque quando você faz backup de dados, ele também captura informações relacionadas ao sistema operacional, aplicativos instalados, drivers e assim por diante.

É possível executar uma BMR por meio de qualquer uma das seguintes opções:

- Usando a opção de linha de comando. Para obter detalhes, consulte Criar um modelo de configuração usando a linha de comando.
- Usando o endereço IP ou o endereço MAC (Media Access Control – Controle de Acesso ao Meio) do computador de destino. Se você inicializar o computador de destino usando o Live CD do Agente do Arcserve UDP (Linux), será possível obter o endereço IP do computador de destino.

  Observação: a máquina pode ser inicializada. Há apenas um NIC configurado.

O diagrama a seguir exibe o processo para executar uma BMR usando o endereço IP ou MAC:



Conclua as tarefas a seguir para executar uma BMR:

- Verificar os pré-requisitos da BMR
- Obter o endereço IP do computador de destino usando o Live CD
- (Opcional) Recuperar dados para o volume iSCSI do computador de destino
- (Opcional) Recuperar dados do volume iSCSI para o computador de destino
- Analisar o servidor de backup
- Especificar os pontos de recuperação
- Especificar os detalhes da máquina de destino
- Especificar as configurações avançadas
- (Opcional) Gerenciar scripts anteriores e posteriores para automação
- Criar e executar a tarefa de restauração
- (Opcional) Executar as operações pós-BMR
- Verificar se a máquina de destino foi restaurada

Criar um modelo de configuração usando a linha de comando

Crie um arquivo de configuração para que o comando d2dbmr possa restaurar as VMs de acordo com os parâmetros especificados no arquivo. O arquivo d2dbmr reúne todas as especificações do arquivo e executa a restauração de acordo com as especificações. O comando d2dbmr é usado para executar a BMR pela linha de comando.

Sintaxe

d2dbmr --createtemplate=[save path]

O utilitário d2dutil --encrypt criptografa a senha e fornece uma senha criptografada. Você deve usar esse utilitário para criptografar todas as suas senhas. Se você usar o parâmetro --pwdfile=pwdfilepath, deve criptografar a senha. É possível usar o utilitário por meio de um dos seguintes métodos:

Método 1

```
echo 'string' | ./d2dutil --encrypt
```

string é a senha que você especificar.

Método 2

Digite o comando "d2dutil –encrypt" e, em seguida, especifique sua senha. Pressione Enter e verá o resultado na tela. Nesse método, a senha que digitar não será reproduzida na tela.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie o modelo de configuração usando o seguinte comando:

   ```
   d2dbmr --createtemplate=[save path]
   ```

   [save path] indica o local em que o modelo de configuração é criado.
3. Abra o modelo de configuração e atualize os seguintes parâmetros:

   job_name

   Especifica o nome da tarefa de restauração.

   storage_location_type

   Especifica o tipo de local do armazenamento da sessão. O local de armazenamento pode ser CIFS, NFS ou RPS.

   storage_location

Especifica o local do servidor de armazenamento da sessão. O local de armazenamento pode ser CIFS ou NFS.

storage_username

Especifica o nome de usuário quando você usa o CIFS como local de armazenamento.

storage_password

Especifica a senha quando você usa o CIFS como local de armazenamento. A senha é criptografada usando o utilitário de criptografia d2dutil.

rps_server

Especifica o nome do servidor de ponto de recuperação quando **storage_location_type** é RPS.

rps_server_username

Especifica o nome de usuário do servidor do ponto de recuperação quando **storage_location_type** é RPS.

rps_server_password

Especifica a senha do servidor do ponto de recuperação quando **storage_location_type** é RPS. A senha é criptografada usando o utilitário de criptografia d2dutil.

rps_server_protocol

Especifica o protocolo do servidor de ponto de recuperação quando **storage_location_type** é RPS.

rps_server_port

Especifica a porta do servidor do ponto de recuperação quando **storage_location_type** é RPS.

rps_server_datastore

Especifica o nome do repositório de dados do servidor de ponto de recuperação quando **storage_location_type** é RPS.

encryption_password

Especifica a senha de criptografia da sessão. A senha é criptografada usando o utilitário de criptografia d2dutil.

source_node

Especifica o nome da origem do nó cujo ponto de recuperação é usado para a restauração.

recovery_point

Especifica a sessão que você deseja restaurar. Em geral, uma sessão de recuperação está no seguinte formato: S00000000X, em que X é um valor numérico. Se desejar restaurar a sessão mais recente, especifique a palavra-chave “last”.

exclude_volumes

Especifica os volumes a serem excluídos para a VM de destino.

Não exclua o volume ‘/’. Use ':' para separar vários volumes.

include_volumes

Especifica os volumes a serem incluídos na VM de destino.

Deve incluir os seguintes volumes: / , /boot , /boot/efi , /home , /usr , /usr/-local. Use ':' para separar vários volumes.

restore_target

Especifica o endereço MAC/IP do destino da restauração.

guest_hostname

Especifica o nome do host que você deseja fornecer depois de restaurar a VM.

guest_network

Especifica o tipo de rede que você deseja configurar. A rede pode ser DHCP ou estática.

guest_ip

Especifica o endereço IP quando você especifica o IP estático.

guest_netmask

Especifica a máscara da rede quando você especifica o IP estático.

guest_gateway

Especifica o endereço de gateway quando você especifica o IP estático.

guest_dns

Especifica o endereço DNS quando você especifica o IP estático.

guest_reboot

(Opcional) Especifica se a VM de destino deve ser reiniciada depois que a VM for restaurada. Os valores são yes e no.

Padrão: no

guest_reset_username

(Opcional) Especifica para redefinir a senha para o valor que você fornece no parâmetro guest_reset_ password.

guest_reset_password

(Opcional) Especifica para redefinir a senha para o valor especificado. A senha é criptografada usando o utilitário de criptografia d2dutil.

enable_instant_restore

(Opcional) Especifica a ativação da restauração instantânea. Os valores são yes e no.

auto_restore_data

(Opcional) Especifica a restauração automática dos dados. Os valores são yes e no.

script_pre_job_server

(Opcional) Especifica o script a ser executado antes da execução da tarefa no servidor.

script_post_job_server

(Opcional) Especifica o script a ser executado depois da execução da tarefa no servidor.

script_pre_job_client

(Opcional) Especifica o script a ser executado antes da execução da tarefa no cliente.

script_post_job_client

(Opcional) Especifica o script a ser executado após a execução da tarefa no cliente.

script_ready_to_use

(Opcional) Especifica o script a ser executado quando o computador de destino está pronto para uso e o valor do parâmetro **enable_instant_restore** é Sim.

force

Especifica se é necessário forçar a restauração da VM. Os valores são yes e no.

Padrão: no

4. Salve e feche o modelo de configuração.

   O modelo de configuração foi criado com êxito.

5. Envie uma tarefa usando o modelo d2dbmr com o seguinte comando:

./d2dbmr –template=cfg_file_path [--wait]

Observação: a opção --wait permite retornar ao ambiente do shell após a conclusão da tarefa de restauração. Se a opção --wait não estiver disponível, volte imediatamente ao ambiente do shell depois de enviar a tarefa.

A tarefa de restauração será enviada.

Verificar os pré-requisitos da BMR

Considere as seguintes opções antes de executar uma BMR:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Você tem um computador de destino válido para a BMR.
- Certifique-se de que criou o Live CD do Agente do Arcserve UDP (Linux).
- Se você deseja executar uma BMR usando o endereço IP, deve obter o endereço IP do computador de destino usando o Live CD.
- Se você deseja executar uma BMR com base em PXE usando o endereço MAC, deve ter o endereço MAC do computador de destino.
- Quando o destino de backup de uma tarefa de backup é o local de origem, para executar uma tarefa de BMR do destino é necessário exportar do destino do local de origem por meio de NFS ou CIFS e especificar o ponto de recuperação como disponível no compartilhamento NFS ou CIFS.
- O ponto de recuperação deve ser proveniente do backup com base em agente do Linux.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Obter o endereço IP do computador de destino usando o Live CD

Antes de executar uma BMR usando o endereço IP, é necessário obter o endereço IP do computador de destino. O computador bare metal não tem um endereço IP inicial. Portanto, você precisa inicializar o computador bare-metal usando o Live CD padrão, que é o Live CD do Agente do Arcserve UDP (Linux), ou o Live CD com base no CentOS para obter o endereço IP. Após obter o endereço IP do computador de destino, é possível configurar o IP estático do computador de destino.

Siga estas etapas:

1. Insira o Live CD ou monte o arquivo .iso do Live CD na unidade de CD-ROM do nó de destino.
2. Inicialize o computador de destino a partir do CD-ROM.

   O computador de destino é inicializado no ambiente do Live CD do Agente do Arcserve UDP (Linux). O endereço IP do computador de destino é exibido na tela.

3. Para configurar o IP estático do computador de destino usando o Live CD padrão, siga estas etapas:
   a. Na tela do computador de destino, pressione Enter para inserir o ambiente de shell.
   b. Execute o comando a seguir para configurar o IP estático:

      ```
      ifconfig <nome da NIC>  <endereço IP estático> netmask <máscara de rede>
      ```

      ```
      adição de rota padrão  gw  <endereço IP do gateway> <nome da NIC>
      ```

      Observação: o nome da NIC (Network Interface Card - Placa de Interface de Rede) depende de seu hardware. Por exemplo, os nomes típicos da NIC são eth0 ou em0.

4. Para configurar o IP estático do computador de destino usando o Live CD com base no CentOS, siga estas etapas:
   a. Abra uma janela do terminal no computador de destino clicando em Aplicativos, Ferramentas do sistema, Terminal.
   b. Execute os seguintes comandos:

      ```
      sudo ifconfig <nome da NIC>  <endereço IP estático> netmask <máscara de rede>
      ```

```
sudo route add default  gw  <endereço IP do gateway> <nome da
NIC>
```

Observação: o nome da NIC (Network Interface Card - Placa de Interface de Rede) depende de seu hardware. Por exemplo, os nomes típicos da NIC são eth0 ou em0.

O IP estático é configurado.

O endereço IP do computador de destino é obtido.

Importante: Mantenha um registro desse endereço IP, pois ele será usado no **Assistente de restauração** quando for necessário especificar os detalhes do computador de destino.

(Opcional) Recuperar dados para o volume iSCSI do computador de destino

É possível integrar o volume iSCSI no computador de destino e tornar este volume parte do computador de destino. Em seguida, é possível restaurar os dados para o volume iSCSI do computador de destino. Assim, será possível gerenciar dados e transferi-los por uma rede.

Importante: Ao integrar o volume iSCSI ao computador de destino, você perderá todos os dados existentes do volume iSCSI.

Siga estas etapas:

1. Insira o Live CD do Agente do Arcserve UDP (Linux) ou monte o arquivo ISO do Live CD do Agente do Arcserve UDP (Linux) na unidade de CD-ROM do computador de destino.
2. Inicialize o computador de destino a partir do CD-ROM.

   O computador de destino é inicializado no ambiente do Live CD do Agente do Arcserve UDP (Linux). O endereço IP do computador de destino é exibido na tela.
3. Digite o ambiente do shell do computador de destino.
4. Execute o seguinte comando para iniciar o daemon do iniciador iSCSI:

   ```
   /etc/init.d/iscsid start
   ```
5. Execute um script de detecção para detectar o host de destino iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   O valor da porta padrão do host de destino iSCSI é 3260.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```
6. Anote o IQN (iSCSI Qualified Name – Nome Qualificado iSCSI) do host de destino iSCSI encontrado pelo script de detecção antes de efetuar logon manualmente no destino detectado.
7. Liste o dispositivo de bloqueio disponível do nó de destino.

   ```
   #fdisk -l
   ```

8. Efetue logon no destino detectado.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-
   SERVER-IP-ADDRESS>:<Port_Number> -l
   ```

   É possível ver um dispositivo de bloqueio no diretório /dev do nó de destino.

9. Execute o comando a seguir para obter o novo nó do dispositivo:

   ```
   #fdisk –l
   ```

   É possível ver um dispositivo adicional nomeado /dev/sd<x> no nó de destino.

   O volume iSCSI é integrado ao volume de destino.

(Opcional) Recuperar dados do volume iSCSI para o computador de destino

Se você tiver armazenado os dados em um volume de destino iSCSI, é possível conectar o volume iSCSI e recuperar os dados. O volume iSCSI permite gerenciar dados e transferi-los por uma rede.

Siga estas etapas:

1. Insira o Live CD do Agente do Arcserve UDP (Linux) ou monte o arquivo ISO do Live CD do Agente do Arcserve UDP (Linux) na unidade de CD-ROM do computador de destino.
2. Inicialize o computador de destino a partir do CD-ROM.

   O computador de destino é inicializado no ambiente do Live CD do Agente do Arcserve UDP (Linux). O endereço IP do computador de destino é exibido na tela.
3. Digite o ambiente do shell do computador de destino.
4. Execute o seguinte comando para iniciar o daemon do iniciador iSCSI:

   ```
   /etc/init.d/iscsid start
   ```
5. Execute um script de detecção para detectar o host de destino iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   O valor da porta padrão do host de destino iSCSI é 3260.
6. Anote o IQN (iSCSI Qualified Name – Nome Qualificado iSCSI) do host de destino iSCSI encontrado pelo script de detecção antes de efetuar logon manualmente no destino detectado.
7. Liste o dispositivo de bloqueio disponível do nó de destino.

   ```
   #fdisk -l
   ```
8. Efetue logon no destino detectado.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   É possível ver um dispositivo de bloqueio no diretório /dev do nó de destino.
9. Execute o comando a seguir para obter o novo nome do dispositivo:

   ```
   #fdisk -l
   ```

É possível ver um dispositivo adicional nomeado /dev/sd<x> no nó de destino.

Por exemplo, considere que o nome do dispositivo é /dev/sdc. Esse nome de dispositivo é usado para criar uma partição e um sistema de arquivos nas etapas a seguir.

10. Monte o volume iSCSI usando os seguintes comandos:

```
# mkdir /iscsi
```

```
# mkdir /iscsi
```

Observação: ao especificar o local da sessão no Assistente de restauração, é necessário selecionar Local e digitar o caminho /iscsi.

Exemplo: <path>/iscsi

O computador de destino agora pode se conectar ao volume iSCSI e pode recuperar os dados do volume iSCSI.

Analisar o servidor de backup

Ao abrir o **Assistente de restauração**, verifique o servidor de backup no qual deseja executar a operação de restauração.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   - A partir do Arcserve UDP:

   a. Clique na guia **Recursos**.

   b. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   c. No painel central, selecione o nó do e clique em **Ações**.

   d. Clique em **Restaurar** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve UDP (Linux) é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   e. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   - A partir do Agente do Arcserve UDP (Linux):

   a. Abra a interface da web do Agente do Arcserve UDP (Linux).

      Observação: durante a instalação do Agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor. Efetue logon no Agente do Arcserve UDP (Linux)

   b. Clique em **Restaurar** no menu **Assistente**, selecione **Recuperação bare metal (BMR)**.

   A página **Servidor de backup** do **Assistente de restauração – BMR** é exibida.

2. Verifique o servidor na lista suspensa **Servidor de backup** na página **Servidor de backup**.

   Não é possível selecionar nenhuma opção na lista suspensa **Servidor de backup**.

3. Clique em **Avançar**.

   A página **Pontos de recuperação** do **Assistente de restauração – BMR** é exibida.

O servidor de backup é especificado.

Especificar os pontos de recuperação

Cada vez que você executar um backup com êxito, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no **Assistente de restauração** de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

Importante: para executar uma BMR a partir de um ponto de recuperação, o volume raiz e o volume de inicialização devem estar presentes no ponto de recuperação.

Siga estas etapas:

1. Execute uma das seguintes etapas, dependendo do armazenamento de backup.

   - Execute as seguintes etapas para acessar os pontos de recuperação, caso os pontos de recuperação estejam armazenados em um dispositivo móvel:

   a. Inicie o computador de destino usando o Live CD.

   b. Efetue logon na interface da web do Agente do Arcserve UDP (Linux) pelo Live CD.

   c. Abra o **Assistente de BMR**.

   d. Vá até à página **Pontos de recuperação**.

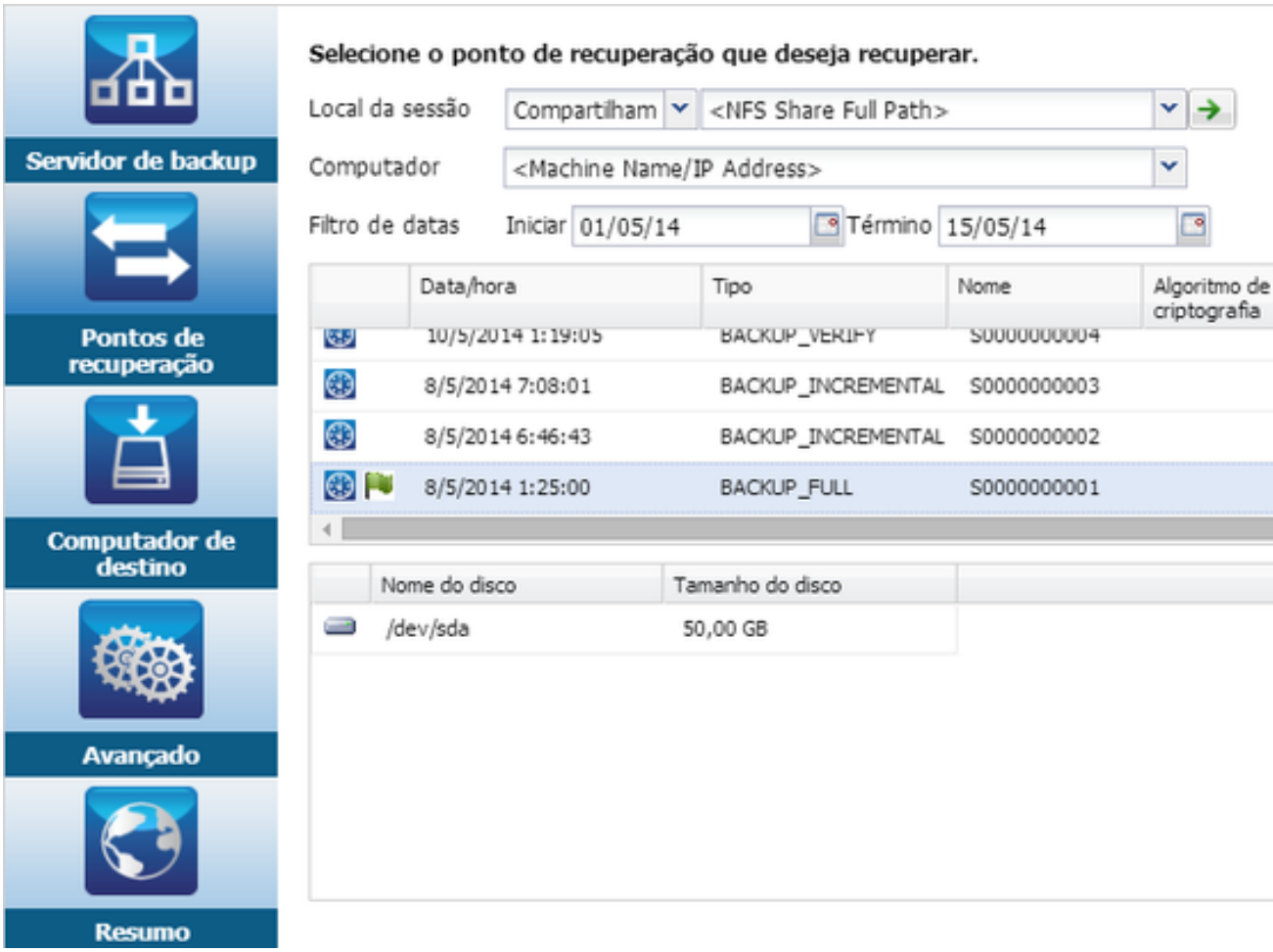
   e. Selecione **Local** como **Local da sessão** na página **Pontos de recuperação** do **Assistente de BMR**.

   - Execute as seguintes etapas se o local da sessão for compartilhamento de NFS ou compartilhamento CIFS:

   a. Selecione uma sessão na lista suspensa **Local da sessão** e digite o caminho completo do compartilhamento.

      Por exemplo, considere o local da sessão como o compartilhamento de NFS, xxx.xxx.xxx.xxx como o endereço IP do compartilhamento de NFS e o nome da pasta como *Dados.* Você deve inserir xxx.xxx.xxx.xxx:/Data como o local de compartilhamento de NFS.

      Observação: se os dados de backup forem armazenados no local de origem, será necessário primeiro converter o nó de origem para um servidor do NFS e, em seguida, compartilhar o local da sessão.



2. Clique em **Conectar**.

   Todos os nós que foram copiados para backup nesse local são listados na lista suspensa **Computador**.

3. Selecione o nó que deseja restaurar na lista suspensa **Computador**.

   Todos os pontos de recuperação do nó selecionado são listados.

4. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

   Padrão: últimas duas semanas.

   Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

5. Selecione o ponto de recuperação que deseja restaurar.
6. Aplique as configurações de Filtro de volume para o ponto de recuperação selecionado e clique em **OK**.

São exibidos todos os volumes disponíveis presentes nesse nó. É possível incluir/excluir volumes conforme a necessidade.

Observação: não exclua os seguintes volumes: / , /boot, /boot/efi, /home, /usr, /usr/local.

7. Clique em **Avançar**.

   A página **Computador de destino** é exibida.

   O ponto de recuperação é especificado.

Especificar os detalhes da máquina de destino

Especifique os detalhes do computador de destino, de modo que os dados sejam restaurados para esse computador. Um computador de destino é um computador bare metal no qual você irá executar uma BMR. Se fizer a restauração usando o endereço IP, será necessário o endereço IP do computador de destino que você já registrou no início deste processo. Se fizer a restauração usando o endereço MAC, será necessário o endereço MAC do computador de destino.

Siga estas etapas:

1. Forneça o endereço MAC ou o endereço IP do computador de destino no campo **Endereço IP/MAC**.
2. Digite um nome no campo **Nome do host**.

   O computador de destino usará esse nome como o nome do host após a conclusão do processo de restauração.

3. Selecione uma das seguintes opções como a rede:

   DHCP

   Configura automaticamente o endereço IP. Essa é a opção padrão. Use essa opção se tiver um servidor DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuração Dinâmica de Host) para restaurar com a rede DHCP.

   IP estático

   Configura manualmente o endereço IP. Se você selecionar essa opção, digite o **Endereço IP**, a **Máscara de sub-rede** e o **Gateway padrão** da máquina de destino.

   Importante: certifique-se de que o IP estático não seja usado por nenhum outro computador da rede durante o processo de restauração.

4. (Opcional) Selecione a opção **Ativar BMR instantânea**, de modo que possa usar a máquina de destino instantaneamente.

   Quando você ativa essa opção, o Agente do Arcserve UDP (Linux) primeiro recupera todos os dados necessários para iniciar a máquina. Os dados restantes serão recuperados depois que a máquina de destino for iniciada. A conexão de rede deve estar sempre disponível durante a BMR instantânea.

   Exemplo: se você tiver 100 GB de dados, desejar executar uma BMR e *não* selecionar essa opção, primeiro, todos os 100 GB de dados serão recuperados e, em seguida, será possível usar a máquina de destino. No entanto, apenas

aproximadamente 1 GB de dados são necessários para iniciar a máquina. Ao ativar essa opção, primeiro, os 1 GB de dados necessários são recuperados, de modo que seja possível iniciar e usar a máquina. Depois que a máquina for iniciada, os 99 GB de dados restantes serão recuperados automaticamente.

Observação: os dados necessários para iniciar a máquina dependem da configuração do sistema operacional. Também é possível pausar ou retomar a recuperação automática de dados se a opção **Não recuperar dados automaticamente depois que o computador for iniciado** não estiver selecionada.

5. (Opcional) Selecione a opção **Não recuperar dados automaticamente quando o computador for iniciado** para interromper a recuperação automática de dados quando a máquina de destino for iniciada.

   Quando você seleciona a opção **Ativar BMR instantânea**, o comportamento padrão é primeiro recuperar os dados necessários e iniciar a máquina. Depois que a máquina for iniciada, os dados restantes são recuperados automaticamente. Se você atualizar os dados de origem durante a recuperação, ao selecionar essa opção, os dados serão recuperados até o ponto antes da atualização.

6. Clique em **Avançar**.

   A página **Avançado** é exibida.

   Os detalhes do computador de destino são especificados.

Especificar as configurações avançadas

Especifique as configurações avançadas para executar uma BMR programada dos dados. A BMR programada garante que os dados sejam recuperados no horário especificado, até mesmo, em sua ausência.

Siga estas etapas:

1. Defina a hora e data de início, selecionando uma das seguintes opções:

   Executar agora

   Inicia a tarefa de restauração assim que você enviar a tarefa.

   Definir horário especial

   Inicia a tarefa de restauração no horário especificado, após enviar a tarefa.

2. (Opcional) Selecione um script a partir da opção **Configurações de scripts anteriores e posteriores** para o servidor de backup e o computador de destino.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos Configurações de scripts anteriores e posteriores serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local:

   `/opt/Arcserve/d2dserver/usr/prepost`

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.

3. (Opcional) Clique em **Mostrar mais configurações** para exibir mais configurações para a BMR.

4. (Opcional) Redefina a senha do nome de usuário especificado para o computador de destino recuperado.

5. (Opcional) Insira o caminho completo do local de armazenamento de backup dos pontos de recuperação no **Acesso local do ponto de recuperação**.

6. (Opcional) Insira o nome completo do disco no campo **Discos** para excluir esses discos no computador de destino da participação no processo de recuperação.

7. (Opcional) Selecione **Ativar o Wake-on-LAN** se estiver executando a BMR de PXE (Preboot Execution Environment – Ambiente de Execução de Pré-inicialização).

Observação: a opção **Ativar o Wake-on-LAN** aplica-se somente às máquinas físicas. Verifique se você ativou as configurações do Wake-on-LAN nas configurações do BIOS da máquina física.

8. (Opcional) Selecione a opção **Reinicialização** para reiniciar automaticamente o nó de destino, após a conclusão da BMR.
9. Clique em **Avançar**.

   A página **Resumo** é exibida.

   As configurações avançadas são especificadas.

(Opcional) Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar os scripts em **Configurações de scripts anteriores e posteriores** do **Assistente de backup** e do **Assistente de restauração** na interface do usuário. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

   Variáveis de ambiente de script anterior e posterior

   Para criar seu script, use as seguintes variáveis de ambiente:

   D2D_JOBNAME

   Identifica o nome da tarefa.

   D2D_JOBID

   Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

   D2D_TARGETNODE

   Identifica o nó cujo backup está sendo feito ou restaurado.

   D2D_JOBTYPE

   Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

   backup.full

   Identifica a tarefa como a tarefa como um backup completo.

   backup.incremental

   Identifica a tarefa como a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino após o início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   ```
   /opt/Arcserve/d2dserver/usr/prepost
   ```

2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.

6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Criar e executar a tarefa de restauração

Crie e execute a tarefa de restauração, para poder iniciar o processo de BMR. Verifique as informações do ponto de recuperação antes de executar uma BMR. Se necessário, será possível voltar e alterar as configurações de restauração.

Siga estas etapas:

1. Verifique os detalhes da restauração na página **Resumo** do **Assistente de restauração**.
2. (Opcional) Clique em **Voltar** para modificar as configurações de restauração em qualquer uma das páginas do **Assistente de restauração.**
3. Digite um nome da tarefa e clique em **Enviar**.

   O campo **Nome da tarefa** tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

   O **Assistente de restauração** é fechado. É possível ver a tarefa na guia **Status da tarefa**. Se você usar o endereço IP para a BMR, o computador de destino será reinicializado automaticamente para o mesmo sistema operacional que a origem do backup, após o processo da BMR.

   Se você usar o endereço MAC para a BMR, o status na guia **Status da tarefa** será alterado para *Aguardando a inicialização do nó de destino*.

4. (Opcional) Para a BMR usando o endereço MAC, inicie o computador de destino quando for exibida a mensagem *Aguardando a inicialização do nó de destino* na guia **Status da tarefa**.

   Observação: se o computador de destino já tiver sido iniciado antes de enviar a tarefa de restauração, é preciso reiniciar o computador de destino. Certifique-se de que o BIOS esteja configurado para inicializar a partir da rede.

   O status na coluna **Status da tarefa** é alterado para **Restaurando o volume**. Isso indica que a restauração está em andamento. Após a conclusão da tarefa de restauração, o computador de destino será reinicializado automaticamente com o mesmo sistema operacional que a origem do backup.

   A tarefa de restauração foi criada e executada com êxito.

(Opcional) Executar as operações pós-BMR

Os tópicos a seguir são configurações opcionais que você pode ter para executar depois de uma BMR:

Configurar o X Windows

Quando você executa uma BMR em um hardware diferente, o X Windows do SO restaurado não funciona corretamente e o nó de destino exibe uma caixa de diálogo de erro. A caixa de diálogo de erro aparece porque a configuração de exibição foi alterada. Para solucionar este problema, siga as instruções da caixa de diálogo de erro para configurar a placa gráfica. Depois disso, você poderá ver o X Windows e a IU da área de trabalho.

Configurar o FQDN (Fully Qualified Domain Name – Nome de Domínio Totalmente Qualificado) do sistema

Quando precisar de um FQDN, terá que configurá-lo. O processo de BMR não configura automaticamente o FQDN.

Contagem máxima de caracteres do FQDN: 63

Siga estas etapas para configurar o FQDN:

1. Edite o arquivo */etc/hosts* e forneça o endereço IP, o nome do FQDN e o nome do servidor.

   ```
   #vi /etc/hosts

   ip_of_system  servername.domainname.com  servername
   ```

2. Reinicie o serviço de rede.

   ```
   #/etc/init.d/network restart
   ```

3. Verifique o nome do host e o nome do FQDN.

   ```
   #hostname

   servername

   #hostname -f

   servername.domainname.com
   ```

O FQDN está configurado.

Estender o volume de dados após uma BMR em discos diferentes

Quando executar uma BMR em um disco maior do que o disco no nó original, algum espaço é deixado sem uso no disco. A operação de BMR não processa automaticamente o espaço em disco não utilizado. É possível formatar o

espaço em disco para uma partição separada ou redimensionar a partição existente com o espaço em disco não utilizado. O volume que você deseja redimensionar não deve estar em uso, por isso, você deve evitar o redimensionamento de um volume do sistema. Nesta seção, o foco será sobre como estender um volume de dados com o espaço em disco não utilizado.

Observação: para evitar a perda de dados, redimensione os volumes imediatamente após o processo de BMR. Também é possível fazer backup do nó antes de iniciar a tarefa de redimensionamento de volume.

Quando o computador de destino reinicia com êxito após a BMR, é possível estender o volume de dados.

Volume de partição bruta

Por exemplo, um disco de 2 GB na sessão é restaurado para um disco de 16 GB nomeado */dev/sdb* com apenas uma partição. A partição bruta */dev/sdb1* é diretamente montada no diretório */data*.

Este exemplo é usado para explicar o procedimento de extensão do volume da partição bruta.

Siga estas etapas:

1. Verifique o status do volume do /dev/sdb1.

```
# df –h /dev/sdb1
/dev/sdb1              2.0G   40M  1.9G   3% /data
```

2. Desmonte o volume do /dev/sdb1.

```
# umount /data
```

3. Redimensione o /dev/sdb1 para ocupar todo o espaço em disco usando o comando fdisk.

   Para executar esta operação, primeiro exclua suas partições existentes e recrie-as com o mesmo número do setor de inicialização. O mesmo número do setor de inicialização é responsável por evitar a perda de dados.

```
# fdisk –u /dev/sdb
Command (m for help): p
Disk /dev/sdb: 17,1 GB, 17179869184 bytes
255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors
Units = sectors of 1 * 512 = 512 bytes
```

```
Device Boot      Start         End      Blocks
Id  System

/dev/sdb1              63     4192964     2096451
83  Linux

Command (m for help): d

Selected partition 1

Command (m for help): n

Command action

e   extended

p   primary partition (1-4)

p

Partition number (1-4): 1

First sector (63-33554431, default 63):

Using default value 63

Last sector or +size or +sizeM or +sizeK (63-
33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdb: 17,1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks
Id  System

/dev/sdb1              63    33554431    16777184+
83  Linux

Command (m for help): w
```

A partição se altera para o mesmo número do setor de inicialização como a partição original e o número do setor de término é 33554431.

4. Redimensione o volume usando o comando resize2fs. Se necessário, execute primeiro o comando e2fsck.

```
# e2fsck -f /dev/sdb1

# resize2fs /dev/sdb1
```

5. Monte o volume para o ponto de montagem e verifique novamente o status do volume.

```
# mount /dev/sdb1 /data

# df –h /dev/sdb1

/dev/sdb1              16G    43M    16G    1% /data
```

O volume é estendido para 16 GB e está pronto para ser usado.

Volume LVM:

Por exemplo, um disco de 8 GB na sessão é restaurado para um disco de 16 GB nomeado */dev/sdc* com apenas uma partição. A partição bruta */dev/sdc1* é usada como o único volume físico do */dev/-mapper/VGTest-LVTest* do volume lógico LVM cujo ponto de montagem é */lvm*.

Esse exemplo é usado para explicar o procedimento de extensão do volume LVM.

Siga estas etapas:

1. Verifique o status do volume /dev/mapper/VGTest-LVTest.

```
# lvdisplay –m /dev/mapper/VGTest-LVTest

# mount /dev/sdb1 /data

--- Logical volume ---

LV Name                /dev/VGTest/LVTest

VG Name                VGTest

LV UUID                udoBIx-XKBS-1Wky-3FVQ-mxMf-
FayO-tpfPl8

LV Write Access        read/write

LV Status              available

# open                 1

LV Size                7.88 GB

Current LE             2018

Segments               1
```

```
Allocation              inherit

Read ahead sectors      0

Block device            253:2

---Segmentos---

Extensão lógica de 0 a 2017:

Type                linear

Physical volume     /dev/sdc1

Physical extents    0 to 2017
```

O volume físico é */dev/sdc1*, o grupo do volume é *VGTest* e o volume lógico é */dev/VGTest/LVTest or /dev/mapper/VGTest-LVTest*.

2. Desmonte o volume /dev/mapper/VGTest-LVTest volume.

```
# umount /lvm
```

3. Desative o grupo do volume no qual o volume físico /dev/sdc1 está localizado.

```
# vgchange -a n VGTest
```

4. Crie uma partição para ocupar o espaço em disco não utilizado usando o comando fdisk.

```
# fdisk -u /dev/sdc

Command (m for help): pDisk /dev/sdc: 17.1 GB,
17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks
Id  System

/dev/sdc1              63    16777215     8388576+
83  Linux

Command (m for help): n

Command actione   extended

p   primary partition (1-4)
```

```
p

Partition number (2-4): 1

First sector (16777216-33554431, default
16777216):

Using default value 16777216

Last sector or +size or +sizeM or +sizeK
(16777216-33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdc: 17,1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks
Id  System

/dev/sdc1              63    16777215     8388576+
83  Linux

/dev/sdc2        16777216    33554431     8388608
83  Linux

Command (m for help): w
```

A partição /dev/sdc2 é criada.

5. Crie um novo volume físico.

```
# pvcreate /dev/sdc2
```

6. Estenda o tamanho do grupo do volume.

```
# vgextend VGTest /dev/sdc2
```

7. Ative o grupo do volume que você já havia desativado.

```
# vgchange -a y VGTest
```

8. Estenda o tamanho do volume lógico usando o comando lvextend.

```
# vgchange -a y VGTest# lvextend -L +8G
/dev/VGTest/LVTest
```

9. Redimensione o volume usando o comando resize2fs. Se necessário, execute primeiro o comando e2fsck.

```
# e2fsck -f /dev/mapper/VGTest-LVTest

# resize2fs /dev/mapper/VGTest-LVTest
```

10. Monte o volume para o ponto de montagem e verifique novamente o status do volume.

```
# mount /dev/mapper/VGTest-LVTest /lvm

# lvdisplay -m /dev/mapper/VGTest-LVTest

---Volume lógico---

LV Name                /dev/VGTest/LVTest

VG Name                VGTest

LV UUID                GTP0a1-kUL7-WUL8-bpbM-9eTR-
SVzl-WgA11h

LV Write Access        read/write

LV Status              available

# open                 0

LV Size                15.88 GB

Current LE             4066

Segments               2

Allocation             inherit

Read ahead sectors     0

Block device           253:2

--- Segments ---

Extensão lógica de 0 a 2046:

Type                linear

Physical volume     /dev/sdc1

Physical extents    0 to 2046

Extensão lógica de 2047 a 4065:

Type                linear

Physical volume     /dev/sdc2
```

```
Physical extents     0 to 2018
```

O volume LVM é estendido para 16 GB e está pronto para ser usado.

Verificar se o nó de destino foi restaurado

Após a conclusão da tarefa de restauração, verifique se o nó de destino foi restaurado com os dados relevantes.

Siga estas etapas:

1. Navegue para o computador de destino que você restaurou.
2. Verifique se o computador de destino possui todas as informações incluídas no backup.

O computador de destino é verificado com êxito.

A BMR é executada com êxito para computadores Linux.

Como executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal) para computadores Linux na nuvem da AWS

Uma BMR restaura o sistema operacional e os aplicativos de software e recupera todos os dados incluídos no backup. A BMR é o processo de restauração de um sistema de computador do estado *bare metal*. Bare metal é um computador sem sistema operacional, drivers e aplicativos de software. Depois que a restauração for concluída, o computador de destino será reinicializado automaticamente no mesmo ambiente operacional que o nó de origem do backup e todos os dados serão restaurados.

Uma BMR completa é possível porque quando você faz backup de dados, ele também captura informações relacionadas ao sistema operacional, aplicativos instalados, drivers e assim por diante.

Você pode executar uma BMR usando o endereço IP da instância de destino do Linux no Amazon EC2. Se você inicializar a instância de destino do Linux usando a AMI do agente do Arcserve UDP (Linux), poderá obter o endereço IP privado da instância.

O processo para realizar uma BMR para instâncias de Linux no Amazon EC2 é praticamente igual ao usado com computadores Linux no local.

Conclua as tarefas a seguir para executar uma BMR:

- Verificar os pré-requisitos da BMR
- Iniciar uma instância usando o Live CD do Agente do Arcserve UDP
- Analisar a instância do servidor de backup
- Especificar os pontos de recuperação
- Especificar os detalhes da instância de destino
- Especificar as configurações avançadas
- Criar e executar a tarefa de restauração
- Verificar se a instância de destino foi restaurada

Verificar os pré-requisitos da BMR

Considere as seguintes opções antes de executar uma BMR para instâncias de Linux no Amazon EC2:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Quando o destino de backup de uma tarefa de backup é o local de origem, para executar uma tarefa de BMR do destino é necessário exportar do destino do local de origem por meio de NFS ou CIFS e especificar o ponto de recuperação como disponível no compartilhamento NFS ou CIFS.
- O ponto de recuperação deve ser proveniente do backup com base em agente do Linux.
- Você tem uma instância do agente do Arcserve UDP para Linux no Amazon EC2.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Iniciar uma instância usando o Live CD do Agente do Arcserve UDP

Antes de executar uma BMR para instâncias de Linux no Amazon EC2, você precisa iniciar uma instância de destino de BMR usando o Live CD do agente do Arcserve UDP. Quando a instância de BMR de destino estiver pronta, obtenha o endereço IP da instância e execute uma tarefa de BMR com o endereço IP.

Siga estas etapas:

1. Efetue logon no console de gerenciamento do EC2 com sua conta e selecione **Iniciar instância**.
2. Selecione uma AMI (Amazon Machine Image) em Community AMIs.

   Você pode pesquisar a Live CD AMI como *Arcserve_UDP_Agent_Linux-LiveCD* em Community AMIs.

   Observações:

   - Se PVM for o nó de origem do backup que você deseja restaurar, selecione o AMI Arcserve_UDP_Agent_Linux-LiveCD-PVM-UDP$version para iniciar a instância.
   - Se HVM ou outra máquina de destino for o nó de origem do backup que você deseja restaurar, selecione Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP$-version AMI para iniciar a instância.
   - O Arcserve_UDP_Agent_Linux-LiveCD-PVM-UDP7.1 é aplicável ao UDP 8.0.
   - O Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP7.2 é aplicável ao UDP 8.0.
3. No assistente de inicialização de instância, selecione o Tipo de instância necessário.
4. Configure os Detalhes da instância quando iniciar outras instâncias. Por exemplo: incluindo Rede, Sub-rede, IP público da atribuição automática ou não, etc.
5. Siga estas etapas para adicionar armazenamento à instância:
   a. Obtenha as informações de disco, incluindo o número e o tamanho do disco do nó de origem do backup que você deseja restaurar. Para obter as informações do disco, você pode selecionar um ponto de recuperação no assistente de restauração para executar uma tarefa de BMR.
   b. Estenda o tamanho do volume raiz para corresponder ao tamanho do disco raiz do nó de origem do backup. Você pode adicionar outros discos existentes no nó de origem do backup.
6. Adicione marcas para a instância de destino de BMR.

7. Siga estas etapas para configurar o grupo de segurança para a instância de destino de BMR:
   a. Crie um grupo de segurança para o tipo SSH.
   b. Para deixar a instância de destino de BMR mais segura, selecione o modo **Personalizado** para a origem que determinará o tráfego que chegará à instância de destino de BMR na regra recém-criada. Especifique a origem personalizada com o formato CIDR para que a instância de destino de BMR fique acessível para o agente do Arcserve UDP para servidor Linux, mas inacessível a outras máquinas da internet.

      Por exemplo, se o IP do agente do Arcserve UDP para Linux for 172.31.X.X, especifique a origem como 172.31.0.0/16 ou 172.0.0.0/8.
8. Revise os detalhes da instância e clique em **Iniciar**.

   A caixa de diálogo **Selecione um par de chaves existente ou crie um novo par** é exibida.
9. Na caixa de diálogo, selecione a opção **Continuar sem um par de chaves** e clique em **Iniciar instâncias**.
10. Obtenha o IP privado na descrição da instância, quando a instância de destino de BMR estiver pronta para uso.

    O endereço IP do computador de destino é obtido.

    Importante: mantenha um registro desse endereço IP, pois ele será usado no **Assistente de restauração** quando for necessário especificar os detalhes da instância de destino de BMR.

Analisar a instância do servidor de backup

Ao abrir o **Assistente de restauração**, verifique a instância do servidor de backup na qual deseja executar a operação de restauração.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   - A partir do Arcserve UDP:

   a. Clique na guia **Recursos**.

   b. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   c. No painel central, selecione o nó do e clique em **Ações**.

   d. Clique em **Restaurar** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve UDP (Linux) é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   e. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   - A partir do Agente do Arcserve UDP (Linux):

   a. Abra a interface da web do Agente do Arcserve UDP (Linux).

      Observação: durante a instalação do Agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor. Efetue logon no Agente do Arcserve UDP (Linux)

   b. Clique em **Restaurar** no menu **Assistente**, selecione **Recuperação bare metal (BMR)**.

   A página **Servidor de backup** do **Assistente de restauração – BMR** é exibida.

2. Verifique o servidor na lista suspensa **Servidor de backup** na página **Servidor de backup**.

   Não é possível selecionar nenhuma opção na lista suspensa **Servidor de backup**.

3. Clique em **Avançar**.

   A página **Pontos de recuperação** do **Assistente de restauração – BMR** é exibida.

O servidor de backup é especificado.

Especificar os pontos de recuperação

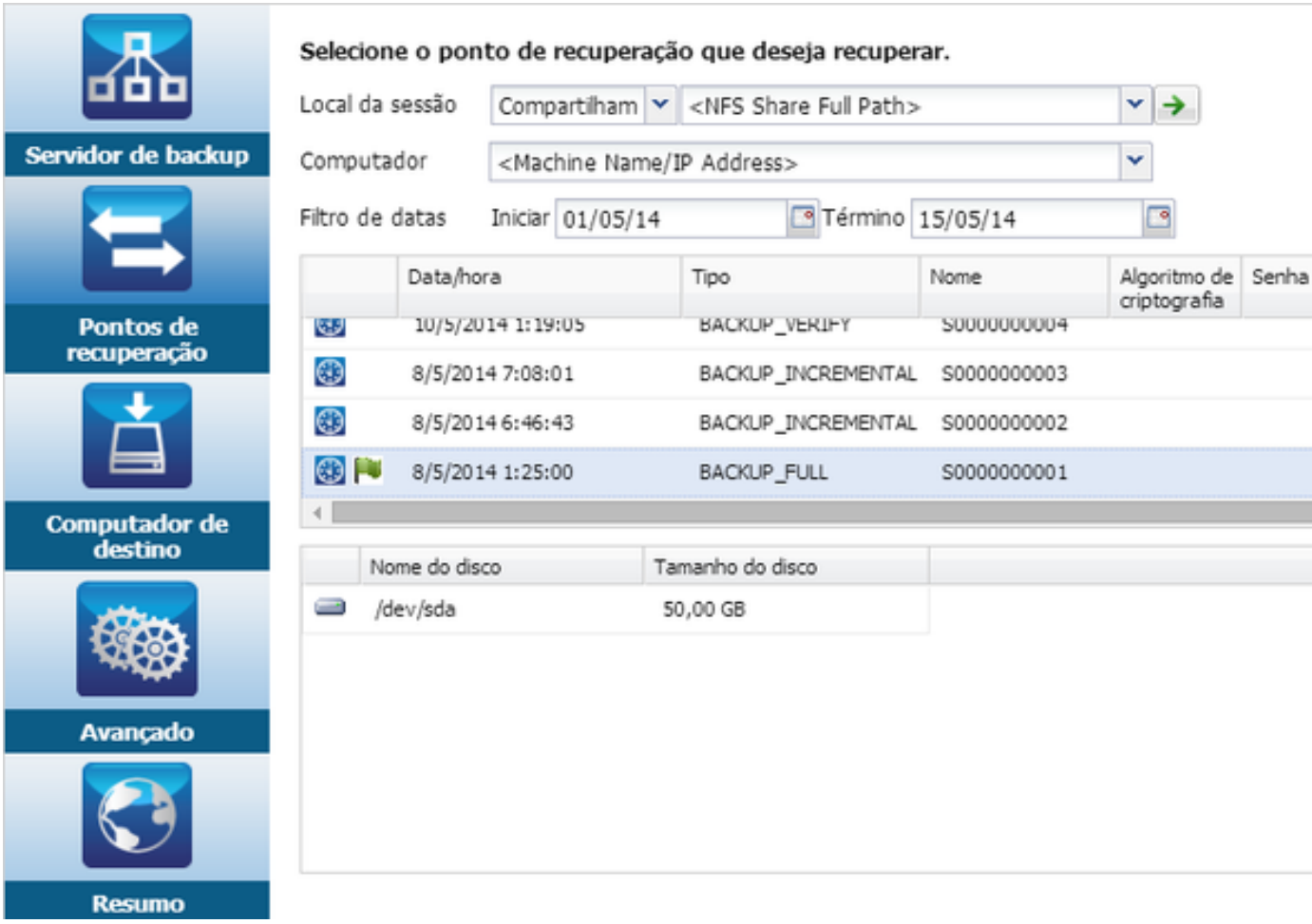
Cada vez que você executar um backup com êxito, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no **Assistente de restauração** de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

Importante: para executar uma BMR a partir de um ponto de recuperação, o volume raiz e o volume de inicialização devem estar presentes no ponto de recuperação.

Siga estas etapas:

1. Selecione uma sessão na lista suspensa **Local da sessão** e digite o caminho completo do compartilhamento.

   Por exemplo, considere o local da sessão como o compartilhamento de NFS, xxx.xxx.xxx.xxx como o endereço IP do compartilhamento de NFS e o nome da pasta como *Dados.* Você deve inserir xxx.xxx.xxx.xxx:/Data como o local de compartilhamento de NFS..



2. Clique em **Conectar**.

   Todos os nós que foram copiados para backup nesse local são listados na lista suspensa **Computador**.

3. Selecione o nó que deseja restaurar na lista suspensa **Computador**.

   Todos os pontos de recuperação do nó selecionado são listados.

4. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

   Padrão: últimas duas semanas.

   Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

5. Selecione o ponto de recuperação que deseja restaurar e clique em **Avançar**.

   A página **Instância de destino de BMR** é exibida.

   O ponto de recuperação é especificado.

Especificar os detalhes da instância de destino

Especifique os detalhes da instância de destino de BMR para restaurar os dados para essa máquina. Uma instância de destino é um computador bare metal no qual você executa uma BMR. Você precisará do endereço IP da instância de destino de BMR registrado no início do processo.

Siga estas etapas:

1. Digite o endereço IP da instância de destino de BMR no campo **Endereço IP/MAC**.
2. Digite um nome no campo **Nome do host**.

   A instância de destino de BMR usa esse nome como o nome do host após a conclusão do processo de restauração.

3. Selecione uma das seguintes opções como a rede:

   DHCP

   Configura automaticamente o endereço IP. Essa é a opção padrão. Use essa opção se tiver um servidor DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuração Dinâmica de Host) para restaurar com a rede DHCP.

   IP estático

   Configura manualmente o endereço IP. Se você selecionar essa opção, digite o **Endereço IP**, a **Máscara de sub-rede** e o **Gateway padrão** da máquina de destino.

   Importante: certifique-se de que o IP estático não seja usado por nenhum outro computador da rede durante o processo de restauração.

4. (Opcional) Selecione a opção **Ativar BMR instantânea**, de modo que possa usar a máquina de destino instantaneamente.

   Quando você ativa essa opção, o Agente do Arcserve UDP (Linux) primeiro recupera todos os dados necessários para iniciar a máquina. Os dados restantes serão recuperados depois que a máquina de destino for iniciada. A conexão de rede deve estar sempre disponível durante a BMR instantânea.

   Exemplo: se você tiver 100 GB de dados, desejar executar uma BMR e *não* selecionar essa opção, primeiro, todos os 100 GB de dados serão recuperados e, em seguida, será possível usar a máquina de destino. No entanto, apenas aproximadamente 1 GB de dados são necessários para iniciar a máquina. Ao ativar essa opção, primeiro, os 1 GB de dados necessários são recuperados, de modo que seja

possível iniciar e usar a máquina. Depois que a máquina for iniciada, os 99 GB de dados restantes serão recuperados automaticamente.

Observação: os dados necessários para iniciar a máquina dependem da configuração do sistema operacional. Também é possível pausar ou retomar a recuperação automática de dados se a opção **Não recuperar dados automaticamente depois que o computador for iniciado** não estiver selecionada.

5. (Opcional) Selecione a opção **Não recuperar dados automaticamente quando o computador for iniciado** para interromper a recuperação automática de dados quando a máquina de destino for iniciada.

   Quando você seleciona a opção **Ativar BMR instantânea**, o comportamento padrão é primeiro recuperar os dados necessários e iniciar a máquina. Depois que a máquina for iniciada, os dados restantes são recuperados automaticamente. Se você atualizar os dados de origem durante a recuperação, ao selecionar essa opção, os dados serão recuperados até o ponto antes da atualização.

6. Clique em **Avançar**.

   A página **Avançado** é exibida.

   Os detalhes da instância de destino de BMR são especificados.

Especificar as configurações avançadas

Especifique as configurações avançadas para executar uma BMR programada dos dados. A BMR programada garante que os dados sejam recuperados no horário especificado, até mesmo, em sua ausência.

Siga estas etapas:

1. Defina a hora e data de início, selecionando uma das seguintes opções:

   Executar agora

   Inicia a tarefa de restauração assim que você enviar a tarefa.

   Definir horário especial

   Inicia a tarefa de restauração no horário especificado, após enviar a tarefa.

2. (Opcional) Selecione um script a partir da opção **Configurações de scripts anteriores e posteriores** para o servidor de backup e a instância de destino de BMR.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos Configurações de scripts anteriores e posteriores serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local:

   `/opt/Arcserve/d2dserver/usr/prepost`

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.

3. (Opcional) Clique em **Mostrar mais configurações** para exibir mais configurações para a BMR.

4. (Opcional) Redefina a senha do nome de usuário especificado para o computador de destino recuperado.

5. (Opcional) Insira o caminho completo do local de armazenamento de backup dos pontos de recuperação no **Acesso local do ponto de recuperação**.

6. (Opcional) Insira o nome completo do disco no campo **Discos** para excluir esses discos na instância de destino de BMR da participação no processo de recuperação.

7. (Opcional) Selecione a opção **Reinicialização** para reiniciar automaticamente o nó de destino, após a conclusão da BMR.

8. Clique em **Avançar**.

   A página **Resumo** é exibida.

As configurações avançadas são especificadas.

(Opcional) Gerenciar scripts anteriores e posteriores para automação na nuvem da AWS

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar os scripts em **Configurações de scripts anteriores e posteriores** do **Assistente de backup** e do **Assistente de restauração** na interface do usuário. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

   Variáveis de ambiente de script anterior e posterior

   Para criar seu script, use as seguintes variáveis de ambiente:

   D2D_JOBNAME

   Identifica o nome da tarefa.

   D2D_JOBID

   Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

   D2D_TARGETNODE

   Identifica o nó cujo backup está sendo feito ou restaurado.

   D2D_JOBTYPE

   Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

   backup.full

   Identifica a tarefa como a tarefa como um backup completo.

   backup.incremental

   Identifica a tarefa como a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado na instância de destino de BMR após o início da tarefa.

post-job-target

Identifica o script que é executado na instância de destino de BMR após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado na instância de destino de BMR antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado na instância de destino de BMR depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   ```
   /opt/Arcserve/d2dserver/usr/prepost
   ```

2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.

6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Criar e executar a tarefa de restauração

Crie e execute a tarefa de restauração, para poder iniciar o processo de BMR. Verifique as informações do ponto de recuperação antes de executar uma BMR. Se necessário, será possível voltar e alterar as configurações de restauração.

Siga estas etapas:

1. Verifique os detalhes da restauração na página **Resumo** do **Assistente de restauração**.
2. (Opcional) Clique em **Voltar** para modificar as configurações de restauração em qualquer uma das páginas do **Assistente de restauração.**
3. Digite um nome da tarefa e clique em **Enviar**.

   O campo **Nome da tarefa** tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

   O **Assistente de restauração** é fechado. É possível ver a tarefa na guia **Status da tarefa**. Se você usar o endereço IP para a BMR, o computador de destino será reinicializado automaticamente para o mesmo sistema operacional que a origem do backup, após o processo da BMR.

   Observação: se o computador de destino já tiver sido iniciado antes de enviar a tarefa de restauração, é preciso reiniciar o computador de destino. Certifique-se de que o BIOS esteja configurado para inicializar a partir da rede.

   O status na coluna **Status da tarefa** é alterado para **Restaurando o volume**. Isso indica que a restauração está em andamento. Após a conclusão da tarefa de restauração, o computador de destino será reinicializado automaticamente com o mesmo sistema operacional que a origem do backup.

   A tarefa de restauração foi criada e executada com êxito.

(Opcional) Executar as operações pós-BMR

Os tópicos a seguir são configurações opcionais que você pode ter para executar depois de uma BMR:

Estender o volume de dados após uma BMR em discos diferentes

Quando executar uma BMR em um disco maior do que o disco no nó original, algum espaço é deixado sem uso no disco. A operação de BMR não processa automaticamente o espaço em disco não utilizado. É possível formatar o espaço em disco para uma partição separada ou redimensionar a partição existente com o espaço em disco não utilizado. O volume que você deseja redimensionar não deve estar em uso, por isso, você deve evitar o redimensionamento de um volume do sistema. Nesta seção, o foco será sobre como estender um volume de dados com o espaço em disco não utilizado.

Observação: para evitar a perda de dados, redimensione os volumes imediatamente após o processo de BMR. Também é possível fazer backup do nó antes de iniciar a tarefa de redimensionamento de volume.

Quando a instância de destino de BMR reinicia com êxito após a BMR, é possível estender o volume de dados.

Volume de partição bruta

Por exemplo, um disco de 2 GB na sessão é restaurado para um disco de 16 GB nomeado */dev/sdb* com apenas uma partição. A partição bruta */dev/sdb1* é diretamente montada no diretório */data*.

Este exemplo é usado para explicar o procedimento de extensão do volume da partição bruta.

Siga estas etapas:

1. Verifique o status do volume do /dev/sdb1.

   ```
   # df –h /dev/sdb1
   /dev/sdb1              2.0G   40M  1.9G   3% /data
   ```

2. Desmonte o volume do /dev/sdb1.

   ```
   # umount /data
   ```

3. Redimensione o /dev/sdb1 para ocupar todo o espaço em disco usando o comando fdisk.

   Para executar esta operação, primeiro exclua suas partições existentes e recrie-as com o mesmo número do setor de inicialização. O

mesmo número do setor de inicialização é responsável por evitar a perda de dados.

```
# fdisk -u /dev/sdb

Command (m for help): p

Disk /dev/sdb: 17,1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks
Id  System

/dev/sdb1              63     4192964     2096451
83  Linux

Command (m for help): d

Selected partition 1

Command (m for help): n

Command action

e   extended

p   primary partition (1-4)

p

Partition number (1-4): 1

First sector (63-33554431, default 63):

Using default value 63

Last sector or +size or +sizeM or +sizeK (63-
33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdb: 17,1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes
```

```
Device Boot      Start         End      Blocks
Id  System

/dev/sdb1              63    33554431    16777184+
83  Linux

Command (m for help): w
```

A partição se altera para o mesmo número do setor de inicialização como a partição original e o número do setor de término é 33554431.

4. Redimensione o volume usando o comando resize2fs. Se necessário, execute primeiro o comando e2fsck.

```
# e2fsck -f /dev/sdb1

# resize2fs /dev/sdb1
```

5. Monte o volume para o ponto de montagem e verifique novamente o status do volume.

```
# mount /dev/sdb1 /data

# df -h /dev/sdb1

/dev/sdb1             16G   43M   16G   1% /data
```

O volume é estendido para 16 GB e está pronto para ser usado.

Volume LVM:

Por exemplo, um disco de 8 GB na sessão é restaurado para um disco de 16 GB nomeado */dev/sdc* com apenas uma partição. A partição bruta */dev/sdc1* é usada como o único volume físico do */dev/-mapper/VGTest-LVTest* do volume lógico LVM cujo ponto de montagem é */lvm*.

Esse exemplo é usado para explicar o procedimento de extensão do volume LVM.

Siga estas etapas:

1. Verifique o status do volume /dev/mapper/VGTest-LVTest.

```
# lvdisplay -m /dev/mapper/VGTest-LVTest

# mount /dev/sdb1 /data

--- Logical volume ---

LV Name                /dev/VGTest/LVTest

VG Name                VGTest
```

```
LV UUID                udoBIx-XKBS-1Wky-3FVQ-mxMf-
FayO-tpfPl8

LV Write Access        read/write

LV Status              available

# open                 1

LV Size                7.88 GB

Current LE             2018

Segments               1

Allocation             inherit

Read ahead sectors     0

Block device           253:2

---Segmentos---

Extensão lógica de 0 a 2017:

Type                linear

Physical volume     /dev/sdc1

Physical extents    0 to 2017
```

O volume físico é */dev/sdc1*, o grupo do volume é *VGTest* e o volume lógico é */dev/VGTest/LVTest or /dev/mapper/VGTest-LVTest*.

2. Desmonte o volume /dev/mapper/VGTest-LVTest volume.

```
# umount /lvm
```

3. Desative o grupo do volume no qual o volume físico /dev/sdc1 está localizado.

```
# vgchange -a n VGTest
```

4. Crie uma partição para ocupar o espaço em disco não utilizado usando o comando fdisk.

```
# fdisk -u /dev/sdc

Command (m for help): pDisk /dev/sdc: 17.1 GB,
17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors
```

```
Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks
Id  System

/dev/sdc1              63    16777215     8388576+
83  Linux

Command (m for help): n

Command actione   extended

p   primary partition (1-4)

p

Partition number (2-4): 1

First sector (16777216-33554431, default
16777216):

Using default value 16777216

Last sector or +size or +sizeM or +sizeK
(16777216-33554431, default 33554431):

Using default value 33554431

Command (m for help): p

Disk /dev/sdc: 17,1 GB, 17179869184 bytes

255 heads, 63 sectors/track, 2088 cylinders, total
33554432 sectors

Units = sectors of 1 * 512 = 512 bytes

Device Boot      Start         End      Blocks
Id  System

/dev/sdc1              63    16777215     8388576+
83  Linux

/dev/sdc2        16777216    33554431     8388608
83  Linux

Command (m for help): w
```

A partição /dev/sdc2 é criada.

5. Crie um novo volume físico.

```
# pvcreate /dev/sdc2
```

6. Estenda o tamanho do grupo do volume.

```
# vgextend VGTest /dev/sdc2
```

7. Ative o grupo do volume que você já havia desativado.

```
# vgchange -a y VGTest
```

8. Estenda o tamanho do volume lógico usando o comando lvextend.

```
# vgchange -a y VGTest# lvextend -L +8G
/dev/VGTest/LVTest
```

9. Redimensione o volume usando o comando resize2fs. Se necessário, execute primeiro o comando e2fsck.

```
# e2fsck -f /dev/mapper/VGTest-LVTest

# resize2fs /dev/mapper/VGTest-LVTest
```

10. Monte o volume para o ponto de montagem e verifique novamente o status do volume.

```
# mount /dev/mapper/VGTest-LVTest /lvm

# lvdisplay -m /dev/mapper/VGTest-LVTest

---Volume lógico---

LV Name                /dev/VGTest/LVTest

VG Name                VGTest

LV UUID                GTP0a1-kUL7-WUL8-bpbM-9eTR-
SVzl-WgA11h

LV Write Access        read/write

LV Status              available

# open                 0

LV Size                15.88 GB

Current LE             4066

Segments               2

Allocation             inherit

Read ahead sectors     0

Block device           253:2

--- Segments ---
```

```
Extensão lógica de 0 a 2046:
Type                linear
Physical volume     /dev/sdc1
Physical extents    0 to 2046
Extensão lógica de 2047 a 4065:
Type                linear
Physical volume     /dev/sdc2
Physical extents    0 to 2018
```

O volume LVM é estendido para 16 GB e está pronto para ser usado.

Verificar se a instância de destino foi restaurada

Após a conclusão da tarefa de restauração, verifique se a instância de destino foi restaurada com os dados relevantes.

Siga estas etapas:

1. Navegue até a instância de destino de BMR que você restaurou.
2. Verifique se a instância de destino de BMR possui todas as informações incluídas no backup.

   A instância de destino é verificada com êxito.

   Observação: quando a instância de destino de BMR estiver pronta para uso, você poderá modificar o grupo de segurança recém-criado de acordo com suas necessidades de negócios.

   A BMR é executada com êxito para computadores Linux.

Como executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal) em computadores Linux na nuvem do Azure

Uma BMR restaura o sistema operacional e os aplicativos de software e recupera todos os dados incluídos no backup. Depois que a restauração for concluída, o computador de destino será reinicializado automaticamente no mesmo ambiente operacional que o nó de origem do backup e todos os dados serão restaurados.

Uma BMR completa é possível porque quando você faz backup de dados, ele também captura informações relacionadas ao sistema operacional, aplicativos instalados, drivers e assim por diante.

Você pode executar uma BMR usando o endereço IP da máquina virtual Linux de destino no Microsoft Azure. O processo de executar uma BMR em instâncias do Linux na nuvem do Azure é ligeiramente diferente do processo usado com computadores Linux locais.

Conclua as tarefas a seguir para executar uma BMR:

- Verificar os pré-requisitos da BMR
- Criar uma nova máquina no Microsoft Azure como destino da BMR
- Verificar a máquina virtual do servidor de backup
- Especificar os pontos de recuperação
- Especificar os detalhes da máquina virtual de destino
- Especificar as configurações avançadas
- Criar e executar a tarefa de restauração
- Verificar se a instância de destino foi restaurada

Verificar os pré-requisitos da BMR

Considere as seguintes opções antes de executar uma BMR para instâncias do Linux no Microsoft Azure:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Quando o destino de backup de uma tarefa de backup é o local de origem, para executar uma tarefa de BMR do destino é necessário exportar do destino do local de origem por meio de NFS ou CIFS e especificar o ponto de recuperação como disponível no compartilhamento NFS ou CIFS.
- O ponto de recuperação deve ser proveniente do backup com base em agente do Linux.
- Você tem um agente do Arcserve UDP para instância do Linux no Microsoft Azure.
- A BMR na máquina virtual Linux de destino deve ter o mesmo sistema operacional do nó de origem do Linux.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Criar uma nova máquina no Microsoft Azure como destino da BMR

Para a BMR no Azure, o usuário pode executar uma BMR de máquina virtual em uma máquina virtual do Linux com o mesmo sistema Linux diretamente no Azure, em vez de iniciar o nó de destino usando o Live CD do Agente do Arcserve UDP.

Em primeiro lugar, crie uma nova máquina virtual no Azure como nó de destino da BMR. Verifique os pré-requisitos a seguir.

- Prepare uma nova máquina virtual com o mesmo sistema operacional usado na máquina virtual que deseja executar uma BMR.
- Configure o tipo de autenticação como Senha na máquina virtual. Lembre-se do nome de usuário e da senha da máquina virtual.
- Configure o grupo de recursos como o grupo no servidor de backup do Linux que realiza a BMR. Caso contrário, a BMR não conseguirá criar a conexão SSH entre o servidor de backup do Linux e a máquina virtual de destino.

Verificar a máquina virtual do servidor de backup

Para obter mais informações, consulte Verificar o servidor de backup.

Especificar os pontos de recuperação

Para obter mais informações, consulte Especificar os pontos de recuperação.

Especificar os detalhes da máquina virtual de destino

Especifique os detalhes da máquina virtual de destino da BMR para restaurar os dados nessa máquina. Uma máquina virtual de destino é um computador bare metal no qual você executa uma BMR. Você precisará do endereço IP, do nome de usuário e da senha da máquina virtual de destino da BMR registrada no início deste processo.

Siga estas etapas:

1. Na tela Restaurar BMR - Assistente, insira os seguintes detalhes:
   - Digite o endereço IP da máquina virtual de destino da BMR no campo Endereço IP.
   - Digite o nome de usuário e a senha da máquina virtual de destino criada no Azure.
2. Para obter os detalhes da máquina:
   - Digite um nome no campo **Nome do host**.

     A máquina virtual de destino da BMR usa esse nome como o nome do host após a conclusão do processo de restauração.
   - Verifique se o DHCP está selecionado por padrão nas Configurações de rede.

     Observação: somente o DHCP está disponível no Azure. O endereço IP é configurado automaticamente.

     DHCP

     Configura automaticamente o endereço IP. Essa é a opção padrão. Use essa opção se tiver um servidor DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuração Dinâmica de Host) para restaurar com a rede DHCP.
3. (Opcional) Selecione a opção **Ativar BMR instantânea**, de modo que possa usar a máquina de destino instantaneamente.

   Quando você ativa essa opção, o Agente do Arcserve UDP (Linux) primeiro recupera todos os dados necessários para iniciar a máquina. Os dados restantes serão recuperados depois que a máquina de destino for iniciada. A conexão de rede deve estar sempre disponível durante a BMR instantânea.

   Exemplo: se você tiver 100 GB de dados, desejar executar uma BMR e *não* selecionar essa opção, primeiro, todos os 100 GB de dados serão recuperados e, em seguida, será possível usar a máquina de destino. No entanto, apenas

aproximadamente 1 GB de dados são necessários para iniciar a máquina. Ao ativar essa opção, primeiro, os 1 GB de dados necessários são recuperados, de modo que seja possível iniciar e usar a máquina. Depois que a máquina for iniciada, os 99 GB de dados restantes serão recuperados automaticamente.

Observação: os dados necessários para iniciar a máquina dependem da configuração do sistema operacional. Também é possível pausar ou retomar a recuperação automática de dados se a opção **Não recuperar dados automaticamente depois que o computador for iniciado** não estiver selecionada.

4. (Opcional) Selecione a opção **Não recuperar dados automaticamente quando o computador for iniciado** para interromper a recuperação automática de dados quando a máquina de destino for iniciada.

   Quando você seleciona a opção **Ativar BMR instantânea**, o comportamento padrão é primeiro recuperar os dados necessários e iniciar a máquina. Depois que a máquina for iniciada, os dados restantes são recuperados automaticamente. Se você atualizar os dados de origem durante a recuperação, ao selecionar essa opção, os dados serão recuperados até o ponto antes da atualização.

5. Clique em **Avançar**.

   A página **Avançado** é exibida.

   Os detalhes da instância de destino de BMR são especificados.

Especificar as configurações avançadas

Para obter detalhes, consulte Especificar as configurações avançadas.

Criar e executar a tarefa de restauração

Para obter detalhes, consulte Criar e executar a tarefa de restauração.

Verificar se a máquina virtual de destino foi restaurada

Para obter detalhes, consulte Verificar se o nó de destino foi restaurado.

Como executar uma BMR de migração em computadores Linux

Uma BMR de migração é um processo de duas etapas onde os dados primeiro são restaurados em um computador temporário e, em seguida, no computador real. Uma BMR com a opção de BMR instantânea ativada permite recuperar dados para um computador temporário. É possível usar o computador temporário até que o computador real esteja pronto. Quando você tiver o computador real, uma BMR de migração permite migrar dados do computador temporário para o computador real. Durante a realização de uma BMR de migração, todos os dados que você criar no computador temporário são migrados para o computador real.

Observação: é possível executar a BMR de migração com apenas um backup com base em agente. Um backup sem agente não oferece suporte à BMR de migração.

É possível executar uma BMR usando o endereço IP ou o endereço MAC (Media Access Control – Controle de Acesso à Mídia) do computador de destino. Se você inicializar o computador de destino usando o Live CD do Agente do Arcserve UDP (Linux), será possível obter o endereço IP do computador de destino.

Observação: a máquina pode ser inicializada. Há apenas um NIC configurado.

Conclua as tarefas a seguir para executar uma BMR de migração:

- Verifique os pré-requisitos para a BMR de migração
- Executar uma BMR para o computador temporário
- Realizar uma BMR de migração
- Verificar se a máquina de destino foi restaurada

Verifique os pré-requisitos para a BMR de migração

Considere as seguintes opções antes de executar uma BMR de migração:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Você tem um computador de destino válido para a BMR.
- Certifique-se de que criou o Live CD do Agente do Arcserve UDP (Linux).
- Se você deseja executar uma BMR usando o endereço IP, deve obter o endereço IP do computador de destino usando o Live CD.
- Se você deseja executar uma BMR com base em PXE usando o endereço MAC, deve ter o endereço MAC do computador de destino.
- O ponto de recuperação deve ser proveniente do backup com base em agente do Linux.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Executar uma BMR para o computador temporário

Antes de realizar uma BMR de migração, você precisa restaurar dados da origem para um computador temporário. Para restaurar os dados temporariamente, é possível executar uma BMR (Bare Metal Recovery – Recuperação Bare-Metal) para o computador temporário. Depois que o computador temporário estiver pronto para uso, é possível continuar trabalhando no computador temporário.

Quando o computador real estiver pronto, você poderá realizar uma BMR de migração do computador temporário para o computador real.

Observação: para obter mais informações sobre como realizar a BMR, consulte o Como executar uma recuperação bare metal (BMR) para máquinas Linux.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   - A partir do Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve UDP (Linux) é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   f. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   - A partir do Agente do Arcserve UDP (Linux):

   a. Abra a interface da web do Agente do Arcserve UDP (Linux).

      Observação: durante a instalação do Agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor.

   b. Efetue logon no Agente do Arcserve UDP (Linux).

2. Clique em **Restaurar** no menu **Assistente**, selecione **Recuperação bare metal (BMR)**.

   A página **Servidor de backup** do **Assistente de restauração – BMR** é exibida.

3. Forneça todos os detalhes no **Assistente de restauração – BMR** e salve o assistente.
4. Certifique-se de marcar a caixa de seleção **Ativar a BMR instantânea** na página **Computador de destino** do assistente.
5. Certifique-se de marcar a caixa de seleção **Não recuperar os dados automaticamente depois que o computador for iniciado** na página **Computador de destino** do assistente.
6. Execute a tarefa de BMR.

   O computador temporário foi recuperado usando a BMR, com a opção de BMR instantânea ativada. É possível usar o computador temporário até que o computador real esteja pronto.

Realizar uma BMR de migração

Quando o computador real estiver pronto, execute uma BMR de migração. A BMR de migração restaura os dados originais da sessão de backup e os novos dados do computador temporário para o computador real.

Siga estas etapas:

1. Clique em **Restaurar** no menu **Assistente** e selecione **BMR de migração**.

   A página **Servidor de backup** do **Assistente de restauração – BMR de migração** é exibida.

2. Forneça todos os detalhes do **Assistente de restauração – BMR de Migração**.

   Observação: para obter mais informações sobre como realizar a BMR, consulte o Como executar uma recuperação bare metal (BMR) para máquinas Linux.

3. Certifique-se de que as seguintes informações são fornecidas na página **Servidor de Backup** do assistente.

a. Selecione a tarefa de recuperação de VM instantânea ou a tarefa de BMR instantânea.

   Servidor local

   Especifica que o servidor de backup é gerenciado no local. A tarefa de BMR do computador temporário é executada no servidor local.

   Servidor remoto

   Especifica que o servidor de backup é gerenciado remotamente. A tarefa de BMR do computador temporário é executada no servidor remoto. É necessário fornecer os detalhes do servidor remoto para se estabelecer conexão com o servidor remoto.

b. Selecione a tarefa de restauração na lista suspensa Nome da tarefa.

   A lista exibe a tarefa de recuperação de VM instantânea ou a tarefa de BMR instantânea, que está na fase da tarefa Pronto para uso ou na fase da tarefa Desligar, quando ela estiver pronta para uso.

4. Salve a tarefa de BMR.

   Na página inicial, a **Fase da tarefa** na guia **Status da tarefa** muda para **Clique aqui para migrar dados**.

5. (Opcional) Inicialize o computador temporário usando um Live CD quando o tipo de tarefa selecionada for BMR instantânea.

6. Na guia **Status da tarefa**, clique em **Clique aqui para migrar dados**.

   A migração de dados é iniciada.

   Você realizou uma BMR de migração com êxito.

Verificar se o nó de destino foi restaurado

Após a conclusão da tarefa de restauração, verifique se o nó de destino foi restaurado com os dados relevantes.

Siga estas etapas:

1. Navegue para o computador de destino que você restaurou.
2. Verifique se o computador de destino possui todas as informações do computador temporário, incluindo os novos dados criados no computador temporário.

O computador de destino é verificado com êxito.

A BMR de migração é executada com êxito para computadores Linux com base em agente.

Como executar uma BMR de migração em máquinas Linux do Amazon EC2 para um computador local

Uma BMR de migração é um processo de duas etapas onde os dados primeiro são restaurados em um computador temporário e, em seguida, no computador real. Uma BMR com a opção de BMR instantânea ativada permite recuperar dados para um computador temporário. É possível usar o computador temporário até que o computador real esteja pronto. Quando você tiver o computador real, uma BMR de migração permite migrar dados do computador temporário para o computador real. Durante a realização de uma BMR de migração, todos os dados que você criar no computador temporário são migrados para o computador real.

Você pode encontrar um problema local no servidor Linux que implica em certo tempo de inatividade. Nesse caso, é possível aproveitar a sessão de backup para criar uma VM instantânea no Amazon EC2 e usar esse servidor para continuar a fornecer os serviços. Quando o problema local for corrigido, a BMR de migração ajudará você a migrar todos os dados do Amazon EC2 para o computador local, e o servidor local será restaurado para fornecer o serviço necessário novamente.

Observação: é possível executar a BMR de migração com apenas um backup com base em agente. Um backup sem agente não oferece suporte à BMR de migração.

É possível executar uma BMR usando o endereço IP ou o endereço MAC (Media Access Control – Controle de Acesso à Mídia) do computador de destino. Se você inicializar o computador de destino usando o Live CD do Agente do Arcserve UDP (Linux), será possível obter o endereço IP do computador de destino.

Observação: a máquina pode ser inicializada. Há apenas um NIC configurado.

Conclua as tarefas a seguir para executar uma BMR de migração:

- Verifique os pré-requisitos para a BMR de migração
- Realizar uma BMR de migração
- Verificar se a máquina de destino foi restaurada

Verifique os pré-requisitos para a BMR de migração

Considere as seguintes opções antes de executar uma BMR de migração:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Você tem um computador de destino válido para a BMR.
- Certifique-se de que criou o Live CD do Agente do Arcserve UDP (Linux).
- Se você deseja executar uma BMR usando o endereço IP, deve obter o endereço IP do computador de destino usando o Live CD.
- Se você deseja executar uma BMR com base em PXE usando o endereço MAC, deve ter o endereço MAC do computador de destino.
- O ponto de recuperação deve ser proveniente do backup com base em agente do Linux.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Executar uma migração de BMR do Amazon EC2 para o computador local

Antes de realizar uma BMR de migração do Amazon EC2, você precisa restaurar dados da origem para uma instância de EC2. Para restaurar os dados temporariamente, é possível executar uma VM instantânea para a instância de EC2. Depois que a instância de EC2 estiver pronta, é possível continuar a trabalhar na instância.

Quando o computador local real estiver pronto, você poderá realizar uma BMR de migração da instância do Amazon EC2 para a máquina local real.

Observação: para obter mais informações sobre como realizar a BMR, consulte Como executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal) para computadores Linux.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   - A partir do Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve UDP (Linux) é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   f. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   - A partir do Agente do Arcserve UDP (Linux):

   a. Abra a interface da web do Agente do Arcserve UDP (Linux).

      Observação: durante a instalação do Agente do Arcserve UDP (Linux), você recebeu o URL para acessar e gerenciar o servidor.

b. Efetue logon no Agente do Arcserve UDP (Linux).

2. Clique em **Restaurar** no menu **Assistente** e selecione **BMR de migração**.

   A página **Servidor de backup** do **Assistente de restauração – BMR de migração** é exibida.

3. Siga estas etapas e clique em **Avançar**:

   a. Selecione **Servidor remoto** como local do servidor.

   b. Especifique o servidor de backup Linux no Amazon EC2 para se conectar ao servidor.

   c. Insira o nome do host, o nome de usuário, a senha, o protocolo e a porta para o servidor de backup Linux.

   d. Clique em **Atualizar**, selecione a tarefa de restauração na lista suspensa **Nome da tarefa**.

      A lista exibe a tarefa de recuperação de VM instantânea que está na fase **Pronto para uso** ou **Desligar**, quando pronta para uso.

   A seção Pontos de recuperação é exibida.

4. Na seção **Pontos de recuperação**, realize as etapas a seguir e clique em **Conectar**.

   - Especifique o **servidor RPS** que foi criado localmente.
   - Selecione o repositório de dados correspondente.

     A máquina é carregada automaticamente de acordo com a tarefa de VM instantânea.

   - Selecione a sessão e clique em **Avançar**.

   Você é levado automaticamente para a guia **Computador de destino**.

5. Na seção Computador de destino, digite o endereço MAC/IP e clique em **Avançar**.

   Observação: é possível inicializar um computador local com o Live CD para obter o endereço MAC/IP.

   Você é redirecionado para a seção Avançado.

6. Na seção **Avançado**, configure os scripts anteriores e posteriores e clique em Avançar.

   A seção **Resumo** é exibida.

7. Especifique o nome da tarefa e clique em **Enviar**.

   Uma tarefa de BMR é executada no computador inicializado com o Live CD.

8. Na página inicial do agente do Linux, vá para a guia **Status da tarefa** e clique em

Clique aqui para migrar os dados.

Os dados na VM do Amazon EC2 são migrados para o computador local.

Você realizou uma BMR de migração com êxito.

Verificar se o nó de destino foi restaurado

Após a conclusão da tarefa de restauração, verifique se o nó de destino foi restaurado com os dados relevantes.

Siga estas etapas:

1. Navegue para o computador de destino que você restaurou.
2. Verifique se o computador de destino possui todas as informações do computador temporário, incluindo os novos dados criados no computador temporário.

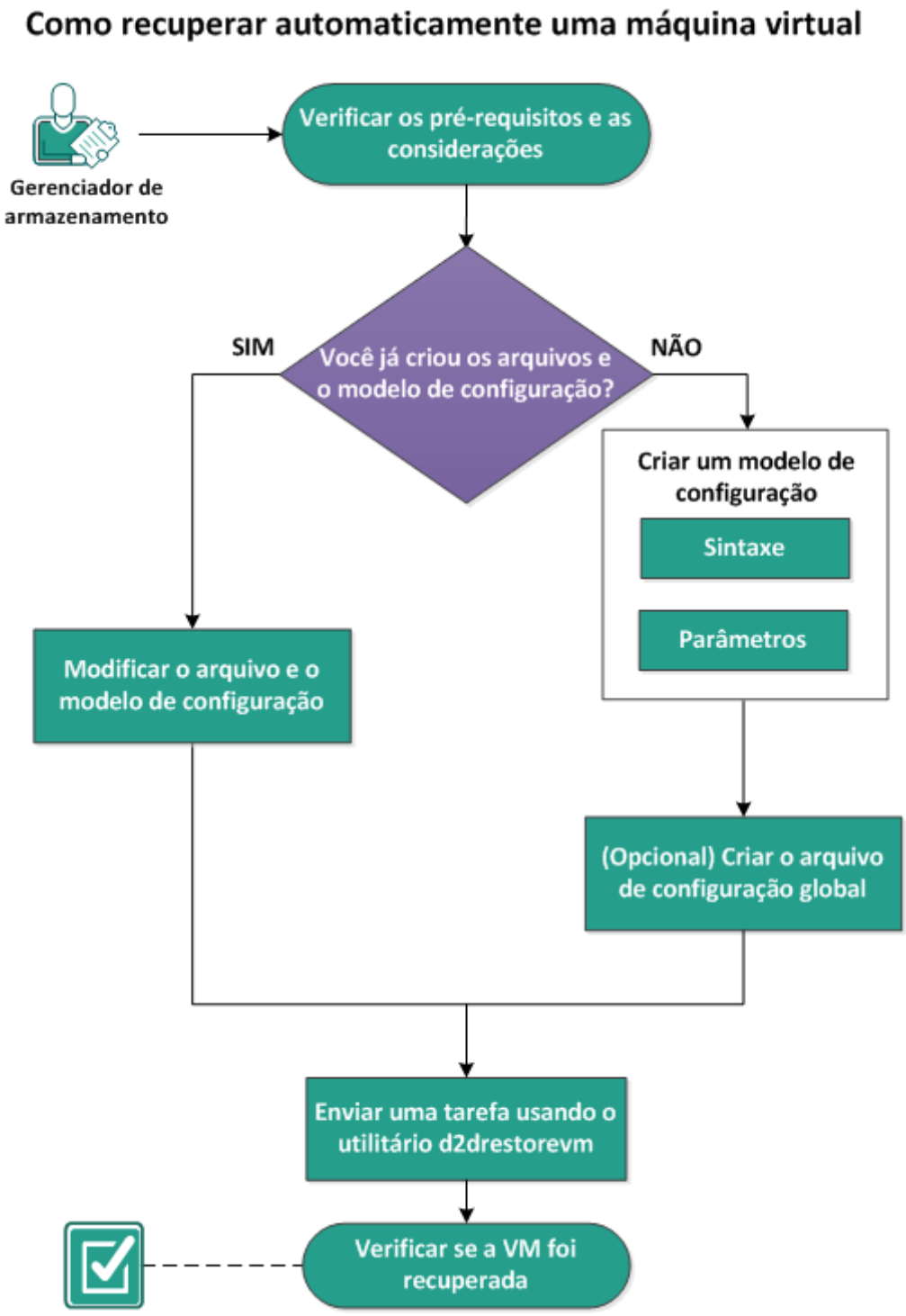
   O computador de destino é verificado com êxito.

   A BMR de migração é executada com êxito para computadores Linux com base em agente.

Como recuperar automaticamente uma máquina virtual

É possível recuperar uma VM (Virtual Machine – Máquina Virtual) a partir da linha de comando do servidor de backup usando o utilitário d2drestorevm. O utilitário d2drestorevm automatiza o processo de execução de uma BMR ou BMR instantânea sem a necessidade de inicializar manualmente a VM usando um Live CD.

O diagrama a seguir mostra o processo para recuperar uma máquina virtual a partir da linha de comando usando o utilitário d2drestorevm:



Execute estas tarefas para recuperar automaticamente uma VM:

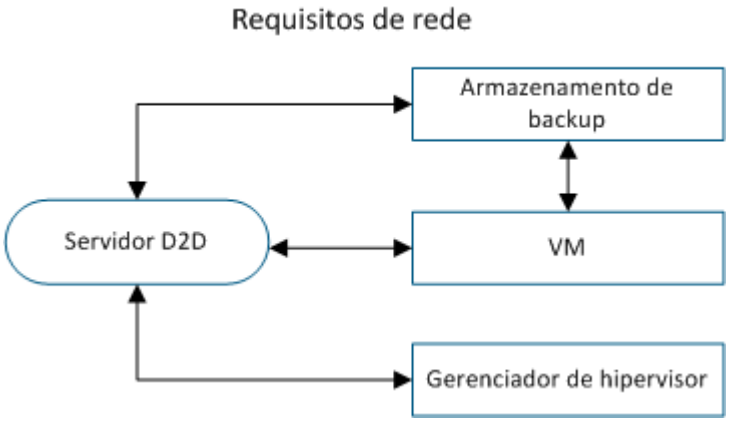
- Verificar os pré-requisitos e as considerações
- Criar um modelo de configuração
- (Opcional) Criar o arquivo de configuração global
- Modificar o arquivo e o modelo de configuração

- Enviar uma tarefa usando o utilitário d2drestorevm
- Verificar se a VM foi recuperada

Verificar os pré-requisitos e as considerações

Verifique os pré-requisitos a seguir antes de restaurar a VM:

- As seguintes versões de hipervisores são suportadas para a BMR ou VM instantânea usando o utilitário d2drestorevm:
  - XenServer 6.0 e posterior (restaurar VM usando o método normal de BMR)
  - OVM 3.2 (restaurar VM usando o método normal de BMR)
  - VMware vCenter/ESX(i) 5.0 ou posterior (enviar tarefa de VM instantânea)
  - Windows Hyper-V server 2012 ou posterior (enviar tarefa de VM instantânea)
  - Nutanix AHV 5.5.3.1 ou posterior (enviar tarefa de VM instantânea)
- Só é possível executar a opção de restauração da VM a partir da linha de comando. Essa opção não está disponível na interface do usuário.
- É possível usar a interface do usuário para monitorar o status da tarefa e os logs de atividades. É possível usar a interface do usuário para pausar, excluir e executar novamente a tarefa de restauração da VM. No entanto, não é possível modificar a tarefa de restauração da VM.
- Antes de restaurar uma VM, é necessário configurar manualmente a VM no Xen, a OVM (Oracle Virtual Machine - Máquina Virtual Oracle).
- Ao restaurar em máquinas virtuais Xen e OVM, é necessário que o servidor NFS esteja instalado e em execução no servidor de backup. Verifique se o firewall não está bloqueando o serviço do NFS e se o hipervisor tem acesso e permissão apropriados para usar o serviço de NFS no servidor de backup.
- Para executar uma restauração da VM bem-sucedida, o hipervisor e a VM de destino devem ter uma conexão de rede válida com o servidor de backup. O diagrama a seguir descreve o requisito de rede:



- O servidor de backup tentará detectar e configurar automaticamente uma NIC virtual para a VM. No entanto, às vezes uma rede válida pode não ser selecionada para a NIC. O parâmetro vm_network permite especificar determinadas redes às quais a NIC deve se conectar. As considerações a seguir são para diferentes plataformas virtuais:
  - No XenServer, após uma instalação, a rede padrão é exibida como Rede 0 no XenCenter, que não é a rede real. Qualquer rede com o nome "Rede de todo o pool associada a xxx" é exibida como "Network 0" no XenCenter. Em tais casos, renomeie a rede padrão e use o novo valor para o parâmetro vm_network.
  - Em OVM, é recomendável configurar manualmente o parâmetro vm_network quando há mais de uma rede disponível.
- Ao usar o compartilhamento CIFS como um local de backup (sessão), considere os seguintes pontos:
  - Use o caractere / em vez de \.
  - Os parâmetros storage_username e storage_password são necessários para verificar as credenciais de compartilhamentos CIFS.
- Pelo menos um dos seguintes parâmetros deve ser especificado para o d2drestorevm funcionar ao restaurar para Xen ou OVM:

  `vm_name`

  `vm_uuid`

  Se ambos os parâmetros forem fornecidos, eles devem pertencer à mesma máquina virtual. Se os parâmetros pertencerem a máquinas virtuais diferentes, ocorrerá um erro.

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Verifique as considerações a seguir antes de restaurar a VM:

- É recomendável restaurar as sessões da release anterior do Agente do Arcserve UDP (Linux) ou Arcserve UDP para Linux para as VMs originais.
- Quando se restaura uma VM em uma PV do XenServer e a VM restaurada exibir uma tela em branco, mas o SSH e outros serviços estiverem ativos, verifique se o parâmetro 'console='kernel está definido corretamente nos argumentos de inicialização.
- Só é possível restaurar as sessões de PV para uma VM de destino de PV no XenServer e OVM.
- HVM de série RHEL 6 e derivativos (RHEL 6, CentOS 6 e Oracle Linux6) podem ser restaurados para uma VM de PV.

Criar um modelo de configuração

Criar um arquivo de configuração para que o comando d2drestorevm possa restaurar as VMs com base nos parâmetros especificados no arquivo. O arquivo d2drestorevm reúne todas as especificações do arquivo e executa a restauração com base nas especificações.

Sintaxe

d2drestorevm --createtemplate=[save path]

O utilitário d2dutil --encrypt criptografa a senha e fornece uma senha criptografada. Você deve usar esse utilitário para criptografar todas as suas senhas. Se você usar o parâmetro --pwdfile=pwdfilepath, deve criptografar a senha. É possível usar o utilitário por meio de um dos seguintes métodos:

Método 1

```
echo 'string' | ./d2dutil --encrypt
```

string é a senha que você especificar.

Método 2

Digite o comando "d2dutil –encrypt" e, em seguida, especifique sua senha. Pressione Enter e verá o resultado na tela. Nesse método, a senha que digitar não será reproduzida na tela.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie o modelo de configuração usando o seguinte comando:

   ```
   d2drestorevm --createtemplate=[save path]
   ```

   [save path] indica o local em que o modelo de configuração é criado.
3. Abra o modelo de configuração e atualize os seguintes parâmetros:

   job_name

   Especifica o nome da tarefa de restauração.

   vm_type

   Especifica o tipo do hypervisor onde restaura a VM. Os tipos de hipervisores válidos são Xen e OVM.

   vm_server

   Especifica o endereço do servidor do hypervisor. O endereço pode ser o nome do host ou o endereço IP.

   vm_svr_username

Especifica o nome de usuário do hypervisor.

vm_svr_password

Especifica a senha do hypervisor. A senha é criptografada usando o utilitário de criptografia d2dutil.

vm_sub_server

Especifica o nome do servidor ESX durante a restauração para o vCenter ou especifica o nome do agrupamento do Prism Element ao fazer a restauração para o Prism Central.

vm_svr_protocol

Especifica o protocolo do hipervisor durante a restauração para o vCenter/ESX(i) ou o AHV.

vm_svr_port

Especifica a porta do hipervisor durante a restauração para o vCenter/ESX(i) ou o AHV.

vm_name

Especifica o nome da máquina virtual de destino exibido no hypervisor.

Importante: O parâmetro vm_name não deve conter nenhum caractere especial, exceto espaços em branco, e deve incluir apenas os seguintes caracteres: a-z, A-Z, 0-9, - e _.

vm_uuid

Especifica a uuid da VM de destino.

vm_network

(Opcional) Especifica o nome da rede que você deseja usar. Se você não fornecer o nome da rede, a rede padrão será selecionada automaticamente.

vm_memory

Especifica a memória da máquina virtual em MB durante a restauração para o vCenter/ESX(i), o Hyper-V ou o AHV.

vm_cpu_count

Especifica a contagem de CPU da máquina virtual durante a restauração para o vCenter/ESX(i), o Hyper-V ou o AHV.

vm_resource_pool

Especifica o pool de recursos do hipervisor durante a restauração para o vCenter/ESX(i) ou o AHV.

vm_datastore

Especifica o repositório de dados do hipervisor durante a restauração para o vCenter/ESX(i) ou o AHV.

storage_location_type

Especifica o tipo de local do armazenamento da sessão. O local de armazenamento pode ser CIFS, NFS ou RPS.

storage_location

Especifica o local do servidor de armazenamento da sessão. O local de armazenamento pode ser CIFS ou NFS.

storage_username

Especifica o nome de usuário quando você usa o CIFS como local de armazenamento.

storage_password

Especifica a senha quando você usa o CIFS como local de armazenamento. A senha é criptografada usando o utilitário de criptografia d2dutil.

rps_server

Especifica o nome do servidor de ponto de recuperação quando **storage_location_type** é RPS.

rps_server_username

Especifica o nome de usuário do servidor do ponto de recuperação quando **storage_location_type** é RPS.

rps_server_password

Especifica a senha do servidor do ponto de recuperação quando **storage_location_type** é RPS. A senha é criptografada usando o utilitário de criptografia d2dutil.

rps_server_protocol

Especifica o protocolo do servidor de ponto de recuperação quando **storage_location_type** é RPS.

rps_server_port

Especifica a porta do servidor do ponto de recuperação quando **storage_location_type** é RPS.

rps_server_datastore

Especifica o nome do repositório de dados do servidor de ponto de recuperação quando **storage_location_type** é RPS.

encryption_password

Especifica a senha de criptografia da sessão. A senha é criptografada usando o utilitário de criptografia d2dutil.

source_node

Especifica o nome da origem do nó cujo ponto de recuperação é usado para a restauração.

recovery_point

Especifica a sessão que você deseja restaurar. Em geral, uma sessão de recuperação está no seguinte formato: S00000000X, em que X é um valor numérico. Se desejar restaurar a sessão mais recente, especifique a palavra-chave "last".

guest_hostname

Especifica o nome do host que você deseja fornecer depois de restaurar a VM.

guest_network

Especifica o tipo de rede que você deseja configurar. A rede pode ser dhcp ou estática.

guest_ip

Especifica o endereço IP quando você especifica o IP estático.

guest_netmask

Especifica a máscara da rede quando você especifica o IP estático.

guest_gateway

Especifica o endereço de gateway quando você especifica o IP estático.

guest_dns

Especifica o endereço DNS quando você especifica o IP estático.

guest_reboot

(Opcional) Especifica se a VM de destino deve ser reiniciada depois que a VM for restaurada. Os valores são yes e no.

Padrão: no

guest_reset_username

(Opcional) Especifica para redefinir a senha para o valor que você fornece no parâmetro guest_reset_ password.

guest_reset_password

(Opcional) Especifica para redefinir a senha para o valor especificado. A senha é criptografada usando o utilitário de criptografia d2dutil.

enable_instant_restore

(Opcional) Especifica a ativação da restauração instantânea. Os valores são yes e no.

auto_restore_data

(Opcional) Especifica a restauração automática dos dados. Os valores são yes e no.

script_pre_job_server

(Opcional) Especifica o script a ser executado antes da execução da tarefa no servidor.

script_post_job_server

(Opcional) Especifica o script a ser executado depois da execução da tarefa no servidor.

script_pre_job_client

(Opcional) Especifica o script a ser executado antes da execução da tarefa no cliente.

script_post_job_client

(Opcional) Especifica o script a ser executado após a execução da tarefa no cliente.

script_ready_to_use

(Opcional) Especifica o script a ser executado quando o computador de destino está pronto para uso e o valor do parâmetro **enable_instant_restore** é Sim.

force

Especifica se é necessário forçar a restauração da VM. Os valores são yes e no.

Padrão: no

exclude_volumes

Especifica os volumes a serem excluídos para a VM de destino.

Não exclua o volume ‘/’. Use ':' para separar vários volumes.

include_volumes

Especifica os volumes a serem incluídos na VM de destino.

Deve incluir os seguintes volumes: / , /boot , /boot/efi , /home , /usr , /usr/-local. Use ':' para separar vários volumes.

4. Salve e feche o modelo de configuração.

   O modelo de configuração foi criado com êxito.

(Opcional) Criar um arquivo de configuração global

O arquivo de configuração global (vm.cfg) tem parâmetros e valores relacionados a locais de armazenamento no qual os discos virtuais da VM são criados. Os valores dos locais de armazenamento são detectados automaticamente durante o processo de restauração. O arquivo vm.cfg substitui os valores relacionados a locais de armazenamento e outros parâmetros. Se desejar especificar um outro local de armazenamento, em vez do valor detectado automaticamente, será possível usar o arquivo vm.cfg.

O arquivo de configuração global está no seguinte local:

`/opt/Arcserve/d2dserver/configfiles/vm.cfg`

É possível configurar os parâmetros a seguir no arquivo vm.cfg:

Parâmetros gerais

D2D_VM_PORT

Permite que você especifique uma porta personalizada para se comunicar com o servidor do hipervisor

- Para OVM, o comando d2drestorevm requer a interface OVM CLI e a porta padrão é 10000.
- Para o XenServer, o comando d2drestorevm se comunica com o servidor usando SSH e a porta padrão é 22.

Parâmetros específicos do OVM

OVM_ISO_REPOSITORY

Permite definir manualmente o repositório para o upload do Live CD do Agente do Arcserve UDP (Linux).

OVM_ISO_UPLOAD_SERVER

Permite especificar manualmente o servidor do repositório para o upload do Live CD do Agente do Arcserve UDP (Linux).

OVM_DISK_REPOSITORY

Permite usar o repositório da OVM específico para criar discos virtuais.

Observação: o utilitário d2drestorevm usa a ID dos parâmetros específicos da OVM.

Parâmetros específicos do Xen

XEN_DISK_SR

Permite usar o repositório de armazenamento XEN específico para criar discos virtuais. O utilitário do d2drestorevm usa o nome de arquivo lexical para parâmetros específicos do RHEV.

Siga estas etapas:

1. Efetue logon no servidor de backup.
2. Crie o arquivo de configuração global e denomine-o como vm.cfg.
3. Abra o arquivo de configuração global e atualize os parâmetros no arquivo.
4. Salve e feche o arquivo
5. Coloque o arquivo na pasta configfiles:

   `/opt/Arcserve/d2dserver/configfiles/vm.cfg`

   O arquivo de configuração global foi criado com êxito.

Modificar o arquivo e o modelo de configuração

Se você já possui o modelo de configuração e o arquivo de configuração global, é possível modificar os arquivos e restaurar outra VM. Você não precisa criar outros modelos e arquivos de configuração cada vez que restaurar uma VM. Ao enviar a tarefa, uma nova tarefa é adicionada à interface do usuário da web. É possível ver os logs de atividades na interface do usuário da web.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o modelo de configuração a partir do local em que você salvou o arquivo e modifique os parâmetros de acordo com as suas necessidades.
3. Salve e feche o modelo de configuração.
4. (Opcional) Abra o arquivo de configuração global a partir do seguinte local e modifique os parâmetros de acordo com suas necessidades:

   ```
   /opt/Arcserve/d2dserver/configfiles/vm.cfg
   ```

5. Salve e feche o arquivo de configuração global.

   O modelo de configuração e o arquivo são modificados com êxito.

Enviar uma tarefa usando o utilitário d2drestorevm

Execute o comando d2drestorevm para restaurar a VM. O comando verifica a VM de destino e envia uma tarefa de restauração. A tarefa de restauração pode ser obtida a partir da interface do usuário da web. Durante o processo de restauração, se qualquer requisito não for atendido, ocorrerá um erro. É possível ver o log de atividades na interface do usuário da web.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Envie a tarefa de restauração para a VM por meio do seguinte comando:

   ```
   d2drestorevm --template=cfg_file_path [--wait]
   ```

   Observação: a opção --wait permite retornar ao ambiente do shell após a conclusão da tarefa de restauração. Se a opção --wait não estiver presente, você retornará ao ambiente do shell imediatamente após enviar a tarefa.

   A tarefa de restauração será enviada.

Verificar se a VM foi recuperada

Após a conclusão da tarefa de restauração, verifique se o nó de destino foi restaurado com os dados relevantes.

Siga estas etapas:

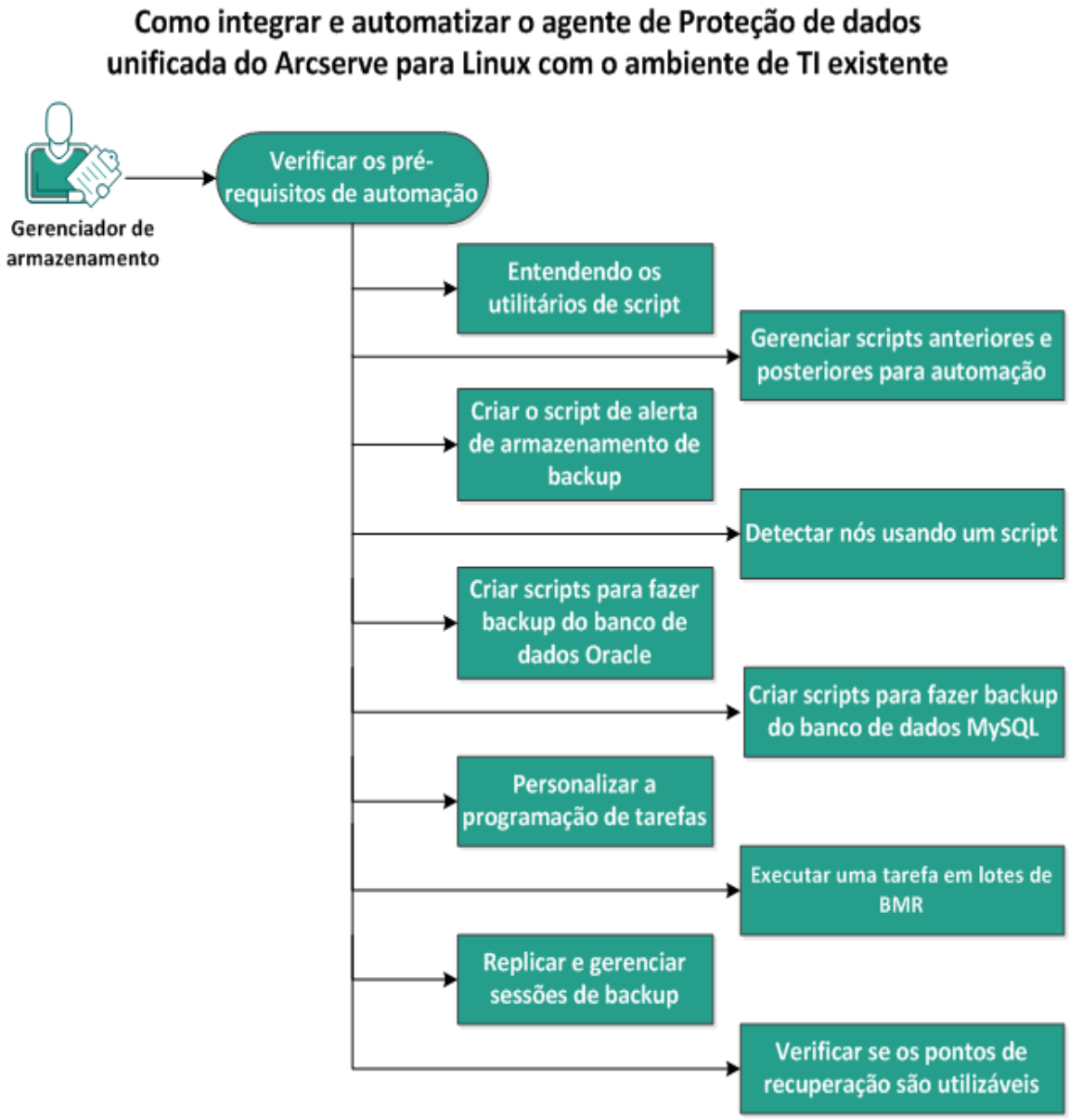
1. Navegue para a VM que você restaurou.
2. Verifique se a VM possui todas as informações incluídas no backup.

   A VM é verificada com êxito.

Como integrar e automatizar o Arcserve UDP para Linux com o ambiente de TI existente

Como gerente de armazenamento, você pode criar scripts e automatizar tarefas para integrar o Agente do Arcserve UDP (Linux) com seu ambiente de TI existente. Os scripts reduzem a intervenção manual e diminuem a dependência na interface da web do servidor de backup para executar qualquer tarefa. O Agente do Arcserve UDP (Linux) também fornece a interface e os utilitários para executar as tarefas de gerenciamento de tarefas, gerenciamento de nós e gerenciamento de log de atividades.

O diagrama a seguir exibe o processo de integração e automação do Agente do Arcserve UDP (Linux) com o ambiente de TI existente:



Execute as seguintes tarefas para automatizar e gerenciar o Agente do Arcserve UDP (Linux):

- Verificar os pré-requisitos de automação
- Entendendo os utilitários de script
- Gerenciar scripts anteriores e posteriores para automação
- Criar o script de alerta de armazenamento de backup
- Detectar nós usando um script
- Criar os scripts para fazer backup do banco de dados Oracle
- Criar os scripts para fazer backup do banco de dados MySQL
- Usar os scripts para fazer backup e restaurar o banco de dados PostgreSQL
- Personalizar a programação de tarefas
- Executar uma tarefa em lotes de BMR
- Replicar e gerenciar sessões de backup
- Verificar se os pontos de recuperação são utilizáveis

Verificar os pré-requisitos de automação

Considere os seguintes pré-requisitos antes de automatizar e gerenciar o Agente do Arcserve UDP (Linux):

- Você possui credenciais de logon raiz para o servidor de backup.
- Deve ter o conhecimento de execução de scripts Linux.
- Você precisa ter um bom conhecimento da interface da web do Agente do Arcserve UDP (Linux).
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Entendendo os utilitários de script

O Agente do Arcserve UDP (Linux) fornece utilitários de script para ajudá-lo a criar seu script de automação. Esses utilitários são simplesmente para execução de scripts, portanto, seus scripts de saída são compatíveis. Os utilitários são usados para gerenciar nós, tarefas, replicar destinos do backup e gerenciar logs de atividades.

Todos os utilitários estão contidos na pasta *bin* no seguinte local:

```
/opt/Arcserve/d2dserver/bin
```

O utilitário d2dutil --encrypt criptografa a senha e fornece uma senha criptografada. Você deve usar esse utilitário para criptografar todas as suas senhas. Se você usar o parâmetro --pwdfile=pwdfilepath, deve criptografar a senha. É possível usar o utilitário por meio de um dos seguintes métodos:

Método 1

```
echo "string" | d2dutil --encrypt
```

a sequência de caracteres é a senha que você especificar.

Método 2

Digite o comando "d2dutil –encrypt" e, em seguida, especifique sua senha. Pressione Enter e verá o resultado na tela. Nesse método, a senha que digitar não será reproduzida na tela.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Navegue para a pasta *bin* usando o seguinte comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

3. Execute os comandos a seguir para gerenciar nós:

   ```
   # ./d2dnode
   ```

   Exibe uma lista dos comandos disponíveis para ajudá-lo a gerenciar todos os nós Linux. Se usar esse comando, será possível adicionar, excluir, modificar e importar nós. Também é possível adicionar nós usando as credenciais não raiz.

   Observação: é possível usar todos os parâmetros do comando d2dnode, quando o servidor de backup for um agente Linux autônomo. Quando o servidor de backup é gerenciado pelo console UDP, o comando d2dnode permite executar somente parâmetros listar, adicionar, modificar e importar. Os parâmetros listar, adicionar, modificar ou importar atualizarão o nó no Console da UDP. Por exemplo, o

comando ./d2dnode --list listará todos os nós do Linux adicionados ao Console do UDP.

```
# ./d2dnode --list lista todos os nós que são gerenciados
pelo servidor de backup.
```

```
# ./d2dnode --add=nodename/ip --user=username --password-
d=password --description="the description of that node" --
attach=jobname --force
```

Adiciona o nó específico ao servidor de backup. Se você for um usuário raiz, use o comando a seguir para adicionar nós.

Observação: se você alterar o número da porta do nó, será necessário especificar o novo número da porta no parâmetro --add conforme mostrado no exemplo a seguir.

Exemplo: # ./d2dnode -–add=nodename/ip:new_port -–user=username -–password-d=password -–description=”the description of that node” --attach=jobname --force

--attach=jobname

Adiciona um novo nó a uma tarefa de backup.

--force

Adiciona o nó de forma forçada mesmo que o nó seja gerenciado por outro servidor de backup. Se você remover o parâmetro *force*, o nó não será adicionado a este servidor se ele for gerenciado por outro servidor de backup.

```
# ./d2dnode --add=nodename -- user=username --
password=password --rootuser=rootaccount --rootpwd-
d=rootpassword --pwdfile=pwdfilepath --des-
cription=description --attach=jobname –force
```

Adiciona o nó específico ao servidor de backup. Se você for um usuário não raiz, use o comando a seguir para adicionar nós.

Observação: se você alterar o número da porta do nó, será necessário especificar o novo número da porta no parâmetro --add conforme mostrado no exemplo a seguir.

Exemplo: # ./d2dnode --add=nodename/ip:new_port --user=username --password-d=password --rootuser=rootaccount --rootpwd=rootpassword --pwdfile=pwdfilepath --description=description --attach=jobname –force

--user=username

Especifica o nome de usuário do usuário não raiz.

--password=password

Especifica a senha do usuário não raiz. Se o parâmetro --pwdfile=pwdfilepath for fornecido, não será necessário especificar esse parâmetro.

--rootuser=rootaccount

Especifica o nome de usuário do usuário raiz.

--rootpwd=rootpassword

Especifica a senha do usuário raiz. Se o parâmetro --pwdfile=pwdfilepath for fornecido, não será necessário especificar esse parâmetro.

--pwdfile=pwdfilepath

(Opcional) Especifica a senha do usuário raiz e do usuário não raiz. Esse parâmetro é opcional, que é usado se você tiver armazenado as senhas de usuário raiz e não raiz em um arquivo separado. O arquivo de senha inclui os seguintes parâmetros: password=password e rootpwd=rootpassword. Para ter mais segurança, a senha deve ser criptografada usando o utilitário d2dutil –encrypt. Após criptografar a senha, substitua a senha antiga pela senha criptografada no parâmetro --pwdfile.

```
# ./d2dnode --node=nodename --attach=jobname
```

Adiciona o nó especificado a uma tarefa de backup existente.

```
# ./d2dnode --modify=nodename/ip --user=username --
password=newpassword --description=newdescription
```

Modifica o nome do usuário, a senha ou a descrição do nó adicionado. Se você for um usuário raiz, use o comando a seguir para modificar nós.

```
# ./d2dnode --modify=nodename -- user=username --
password=newpassword --rootuser=rootaccount --rootpwd-
d=newrootpassword --pwdfile=pwdfilepath --des-
cription=newdescription
```

Modifica o nome do usuário, a senha ou a descrição do nó adicionado. Se você for um usuário não raiz, use o comando a seguir para modificar nós.

--user=username

Especifica o nome de usuário do usuário não raiz.

--password=newpassword

Especifica a nova senha para o usuário que não é raiz.

--rootuser=rootaccount

Especifica o nome de usuário do usuário raiz.

--rootpwd=newrootpassword

Especifica a nova senha do usuário raiz.

--pwdfile=pwdfilepath

(Opcional) Especifica a senha do usuário raiz e do usuário não raiz. Esse parâmetro é opcional, que é usado se você tiver armazenado as senhas de usuário raiz e não raiz em um arquivo separado. O arquivo de senha inclui os seguintes parâmetros: password=newpassword e rootpwd=newrootpassword.

```
# ./d2dnode --delete=nodename1,nodename2,nodename3
```

Exclui os nós especificados do servidor de backup. Para excluir vários nós, use uma vírgula (,) como delimitador.

```
# ./d2dnode --import=network --help
```

Importa nós da rede. Quando você importa os nós, obtém as seguintes opções para configurar:

--netlist

Especifica a lista de endereços IP do IPv4. Para mais de uma entrada, a lista deve ser de entradas separadas por vírgulas.

Exemplo

192.168.1.100: importa o nó que tem o endereço IP 192.168.1.100

192.168.1.100-150: importe todos os nós que pertençam ao escopo (intervalo) entre 192.168.1.100 e 192.168.100.150

192.168.1.100-: importa todos os nós que pertencem ao escopo (intervalo) entre 192.168.1.100 e 192.168.1.254. Aqui, você não precisa mencionar o intervalo final.

192.168.1.100-150,192.168.100.200-250: importa vários nós que pertençam a dois tipos diferentes de escopos. O primeiro escopo (intervalo) está entre 192.168.1.100 e 192.168.1.150 e o segundo escopo está entre 192.168.100.200 e 192.168.100.250. Cada entrada é separada por uma vírgula.

--joblist

Especifica a lista de nomes da tarefa. O nome da tarefa não deve incluir vírgulas. Depois que um nó foi importado com êxito, o nó é adicionado à tarefa. Para mais de uma tarefa, a lista deve ser de entradas separadas por vírgulas.

Exemplo: --joblist=jobA,jobB,jobC

Nesse exemplo, cada entrada de tarefa é separado por uma vírgula.

Observação: essa opção só tem suporte na versão autônoma do Agente do Arcserve UDP (Linux).

--user

Especifica o nome de usuário para importar e adicionar os nós.

--password

Especifica a senha a ser importada e adiciona nós.

--rootuser

Especifica o nome de usuário do usuário raiz. Se um usuário que não seja raiz for adicionado, use esse parâmetro para especificar as credenciais de usuário raiz.

--rootpwd

Especifica a senha do usuário raiz. Se um usuário que não seja raiz for adicionado, use esse parâmetro para especificar as credenciais de usuário raiz.

--pwdfile

(Opcional) Especifica a senha do usuário raiz e do usuário não raiz. Esse parâmetro é opcional, que é usado se você tiver armazenado as senhas de usuário raiz e não raiz em um arquivo separado. O arquivo de senha inclui os seguintes parâmetros: password=newpassword e rootpwd=newrootpassword.

--prefix

Especifica o prefixo fornecido a um nome de host. Use esse parâmetro para filtrar os nós que incluem o prefixo no nome do host.

--blacklistfile

Especifica um arquivo que inclui uma lista de nome do host do nó que você não deseja adicionar ao servidor de backup. Você deve fornecer um nó por linha no arquivo.

--force

Adiciona o nó de forma forçada mesmo que o nó seja gerenciado por outro servidor de backup. Se você remover o parâmetro *force*, o nó não será adicionado a este servidor se ele for gerenciado por outro servidor de backup.

--verbose

Exibe mais informações sobre o processo de importação de nós. Use esse parâmetro para fins de depuração ou scripts de automação.

--help

Exibe a tela de ajuda.

Observações:

- A função de importação usa o servidor SSH para detectar se um nó é um nó Linux. Se o seu servidor SSH usar a porta não padrão, configure o servidor para usar a porta não padrão. Para obter mais informações sobre como configurar o número de porta SSH, consulte Alterar o número de porta SSH do servidor de backup.
- Quando a senha não for fornecida, é usado o método de autenticação de chave de SSH.

4. Execute os seguintes comandos para enviar uma tarefa de restauração de arquivo:

   ```
   d2drestorefile --createtemplate=file
   ```

   Especifica a criação de um modelo. Depois que o modelo é criado, é possível modificá-lo. Esse modelo é usado pelo comando d2drestorefile. Você pode definir os valores nesse modelo. O d2drestorefile lê o modelo e fornece o resultado como especificado no modelo.

   ```
   d2drestorefile --template=restore_template [--wait]
   ```

   Especifica o envio da tarefa de restauração de arquivo. Se você incluir o parâmetro [--wait] no comando, a mensagem de status será exibida após a conclusão da tarefa de restauração.

5. Execute os comandos a seguir para gerenciar tarefas:

   ```
   # ./d2djob
   ```

   Exibe uma lista de comandos para ajudá-lo a gerenciar tarefas. Usando esse comando, você pode executar, cancelar e excluir tarefas

   ```
   # ./d2djob --delete=jobname
   ```

   Exclui a tarefa especificada da guia Status da tarefa.

   ```
   # ./d2djob --run=jobname --jobtype=1 --recoverysetstart --
   wait
   ```

   Executa a tarefa especificada. O parâmetro --jobtype é opcional. O comando d2djob identifica automaticamente o tipo de tarefa a partir do nome da tarefa que você especificar. Se o comando identificar uma tarefa de restauração, a tarefa de restauração será iniciada. Se o comando identificar uma tarefa de backup e não for fornecido nenhum valor para o parâmetro --jobtype, uma tarefa de backup incremental será iniciada. O backup incremental é o tipo de tarefa padrão.

   Se desejar especificar o tipo de tarefa para uma tarefa de backup, os valores são 0, 1 e 2, onde 0 indica uma tarefa de backup completo, 1 indica uma tarefa de backup incremental e 2 indica uma tarefa de backup de verificação.

O parâmetro --recoverysetstart é opcional. Se essa opção for especificada, o backup atual será convertido em backup completo e marcado como o primeiro ponto de recuperação do conjunto de recuperação, se o conjunto de recuperação não estiver disponível.

```
# ./d2djob --cancel=jobname --wait
```

Cancela uma tarefa que está em andamento.

Se você incluir --wait no comando, o status da tarefa será exibido quando a tarefa for cancelada. Se você não incluir --wait no comando, a mensagem de status é exibida imediatamente após enviar a solicitação de cancelamento.

```
# ./d2djob --newrestore=restoreJobName --target=macaddress/ipaddress --hostname=hostname --network=dhcp/staticip --staticip=ipaddress --subnet=subnetMask --gateway=gateway --runnow --wait
```

Executa uma tarefa de restauração para um novo computador de destino com base em uma tarefa de restauração existente. Este comando permite usar as mesmas configurações de restauração da tarefa de restauração existente e apenas os detalhes do computador de destino são diferentes. Se você usar esse comando, não terá que criar várias tarefas de restauração para diferentes computadores de destino.

Você deve fornecer um valor para *--newrestore*, *--target*, *--hostname* e *--network*.

Se o valor de *--network* for staticip, você deve fornecer um valor para *--staticip*, *--subnet* e *--gateway*. Se o valor de *--network* for dhcp, não será necessário fornecer um valor para *--staticip*, *--subnet* e *--gateway*.

Se você incluir --runnow no comando, a tarefa é executada imediatamente após enviar a tarefa, independentemente da programação da tarefa.

Se você incluir o parâmetro --wait no comando, a mensagem de status será exibida após a conclusão da tarefa. Se você não incluir --wait no comando, a mensagem de status é exibida imediatamente após enviar a tarefa.

```
# ./d2djob <--export=jobname1,jobname2,jobname3> <--file=filepath>
```

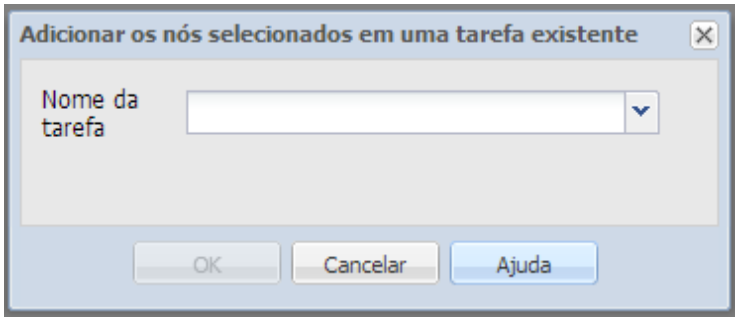
Exporta várias tarefas a partir do servidor de backup para um arquivo. Se desejar as mesmas configurações de backup em vários servidores de backup, será possível exportar as tarefas de backup para um arquivo e importar o arquivo para outros servidores de backup.

Observação: se o servidor de backup Linux for gerenciado pelo console do Arcserve UDP, a função de exportação não terá suporte.

```
# ./d2djob <--import=filepath>
```

Importa o arquivo que contém as informações de tarefas de backup para um servidor de backup. Também será possível importar o arquivo para o Arcserve UDP se o servidor de backup for gerenciado pelo Arcserve UDP.

Se a tarefa de backup for importada para um servidor de backup, será possível selecionar a tarefa na seguinte caixa de diálogo:



Também será possível usar o utilitário de linha de comando a seguir para adicionar nós a essa tarefa:

```
./d2dnode –attach=jobname
```

6. Execute os comandos a seguir para criar ou atualizar o arquivo de configuração de pontos de recuperação. O Agente do Arcserve UDP (Linux) usa o arquivo de configuração para gerenciar e exibir os pontos de recuperação na interface do usuário.

   ```
   # ./d2drp
   ```

   Cria ou atualiza os arquivos de configuração dos pontos de recuperação com base nos detalhes dos pontos de recuperação. Ao usar esse comando, é possível criar ou atualizar os arquivos de configuração.

   ```
   # ./d2drp --build --storagepath=/backupdestination --node-
   e=node_name
   ```

   Verifica todos os pontos de recuperação que pertencem ao *node_name* e atualiza todos os arquivos de configuração dos pontos de recuperação. Se os arquivos de configuração do ponto de recuperação não estiverem presentes, este comando cria os arquivos automaticamente. O parâmetro --build cria os arquivos de configuração dos pontos de recuperação.

   ```
   # ./d2drp --build --storagepath=/backupdestination --node-
   e=node_name --rp=recovery_point
   ```

   Verifica o nome de sessão especificado e atualiza todos os arquivos de configuração dos pontos de recuperação. Se os arquivos de configuração do ponto de recuperação não estiverem presentes, este comando cria os arquivos

automaticamente. Especifique a palavra-chave 'last' para o parâmetro --rp para obter o ponto de recuperação mais recente.

```
# ./d2drp  --show --storagepath=path --node=nodeName --rp=r-
recovery_point --user=username --password=password
```

Exibe as informações do sistema para o ponto de recuperação especificado.

--rp=recovery_point

Selecione o ponto de recuperação que deseja acessar. Especifique a palavra-chave 'last' para obter o ponto de recuperação mais recente.

--user=username

Especifica o nome de usuário para acessar o local de armazenamento ou o destino do backup.

--password=password

Especifica a senha para acessar o local de armazenamento ou o destino do backup.

Observação: para o parâmetro --build, o d2drp não suporta o compartilhamento de NFS nem o compartilhamento CIFS. Se quiser usar o compartilhamento NFS ou o compartilhamento CIFS, é necessário, primeiro, montar o compartilhamento para o host local e, em seguida, usar o ponto de montagem como o caminho de armazenamento.

7. Execute os comandos a seguir para gerenciar logs de atividade:

```
# ./d2dlog
```

Exibe o formato que o ajuda a obter os logs de atividades para a ID da tarefa especificada no formato especificado.

```
# ./d2dlog --show=jobid --format=text/html
```

Exibe o log de atividades da tarefa especificada. O valor do formato é opcional porque o valor padrão é texto.

8. Execute os comandos a seguir para gerenciar o histórico de tarefas:

```
# ./d2djobhistory
```

Exibe o histórico de tarefas com base nos filtros especificados. É possível filtrar o histórico de tarefas por dias, semanas, meses, data de início e data de término.

```
# ./d2djobhistory --day=n --headers=column_name1,column_
name2,...column_name_n --width=width_value --for-
mat=column/csv/html
```

Exibe o histórico de tarefas mais recente com base nos dias especificados.

--headers=column_name1,column_name2,...column_name_n

(Opcional) Especifica as colunas a serem exibidas no histórico de tarefas. Esse é um parâmetro opcional. As colunas predefinidas são ServerName, TargetName, JobName, JobID, JobType, DestinationLocation, EncryptionAlgoName, CompressLevel, ExecuteTime, FinishTime, Throughput, WriteThroughput, WriteData, ProcessedData e Status.

--width=width_value

(Opcional) Especifica o número de caracteres a serem exibidos para cada coluna. Esse é um parâmetro opcional. Cada coluna possui sua própria largura padrão. É possível atualizar o valor de largura de cada coluna, onde cada valor de largura é separado por uma vírgula (,).

--format=column/csv/html

Especifica o formato de exibição do histórico de tarefas. Os formatos disponíveis são coluna, csv e html. É possível especificar somente um formato de cada vez.

```
# ./d2djobhistory --week=n --headers=column_name1,column_
name2,...column_name_n --width=width_value --for-
mat=column/csv/html
```

Exibe o histórico de tarefas mais recente com base nos meses especificados.

```
# ./d2djobhistory --starttime=yyyymmdd --endtime=yyyymmdd
--headers=column_name1, column_name2,...column_name_n --
width=width_value --format=column/csv/html
```

Exibe o histórico de tarefas mais recente com base nas datas de início e de término especificadas.

```
# ./d2djobhistory --starttime=yyyymmdd --endtime=yyyymmdd
--headers=column_name1, column_name2,...column_name_n --
width=width_value --format=column/csv/html
```

Os utilitários de scripts podem ser usados para gerenciar nós, tarefas e logs de atividades com êxito.

Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar seus scripts em **Configurações de scripts anteriores/posteriores** do **Assistente de backup** e do **Assistente de restauração** no console. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

Variáveis de ambiente de script anterior e posterior

Para criar seu script, use as seguintes variáveis de ambiente:

D2D_JOBNAME

Identifica o nome da tarefa.

D2D_JOBID

Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

D2D_TARGETNODE

Identifica o nó cujo backup está sendo feito ou restaurado.

D2D_JOBTYPE

Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

backup.full

Identifica a tarefa como um backup completo.

backup.incremental

Identifica a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino antes do início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

D2D_RECOVERYPOINT

Identifica o ponto de recuperação criado pela tarefa de backup. Esse valor é aplicável no script de backup posterior somente.

D2D_RPSSCHEDULETYPE

Identifica o tipo de programação durante o backup para um repositório de dados no RPS. Os valores a seguir identificam a variável D2D_ RPSSCHEDULETYPE:

diário

Identifica a programação como um backup diário.

semanal

Identifica a programação como um backup semanal.

mensal

Identifica a programação como um backup mensal.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

```
/opt/Arcserve/d2dserver/usr/prepost
```

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   `/opt/Arcserve/d2dserver/usr/prepost`

2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.
6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Exemplo de criação de scripts definidos pelo usuário

A variável de ambiente D2D_JOBSTAGE, que tem quatro estágios diferentes, é muito importante para gravar scripts. No estágio pre_share, você pode fazer algumas preparações ou implementar o método de acesso. No estágio post_share, também é possível implementar o método de acesso, bem como realizar outras ações. A diferença entre os dois estágios é que o caminho indicado da variável D2D_SHARE_PATH está disponível no estágio post_share. Os estágios pre_cleanup e post_cleanup lhe dão a chance de limpar recursos alocados ou quebrar conexões com seu caminho compartilhado. A diferença entre os dois estágios é que o caminho indicado da variável D2D_SHARE_PATH está disponível no estágio pre_cleanup, mas não no estágio post_cleanup.

Observações:

- Você pode ler a senha que definiu para o usuário na IU da web da entrada padrão.
- Seus códigos são executados por processos distintos nos diferentes estágios. Assim, se quiser compartilhar dados em estágios diferentes, você precisará usar um recurso global, como um arquivo ou banco de dados temporário.

Exemplo: criar scripts definidos pelo usuário

Observação: o script SFTP é usado como modelo nos exemplos e no diretório sharerp.

```
#!/bin/bash
function pre_sftp_share()
{
local share_path=${D2D_SHARE_PATH}
local user_name=${D2D_SHARE_USER}
local pass_word=""

# Read pass word from standard input.
read -s pass_word

# Check user whether exist.
if grep $user_name /etc/passwd >/dev/null 2>&1; then
    return 1
fi

# Add new user.
```

```
useradd $user_name -d $share_path >/dev/null 2>&1
[ $? -ne 0 ] && return 2

# Set pass word for the user.
echo -e "$pass_word\n$pass_word"|passwd "$user_name" >/dev/null 2>&1
[ $? -ne 0 ] && return 3

return 0
}

function post_sftp_share()
{
return 0
}

function pre_sftp_cleanup()
{
return 0
}

function post_sftp_cleanup()
{
local user_name=${D2D_SHARE_USER}

# Delete the user.
userdel $user_name >/dev/null 2>&1

return 0
}

# Main
#################################################################
ret=0
stage=${D2D_JOBSTAGE}
case $stage in
pre_share)
pre_sftp_share
ret=$?
```

```
;;

post_share)
post_sftp_share
ret=$?
;;

pre_cleanup)
pre_sftp_cleanup
ret=$?
;;

post_cleanup)
post_sftp_cleanup
ret=$?
;;
esac

exit $ret
```

Criar o script de alerta de armazenamento de backup

Crie o script de alerta de armazenamento de backup de modo que você possa executar o script quando o espaço de armazenamento de backup for menor do que o valor especificado. Quando você adiciona um local de armazenamento de backup na interface de usuário, tem a opção de marcar a caixa de seleção Enviar alerta. Quando você marca a caixa de seleção, o Agente do Arcserve UDP (Linux) monitora o espaço de armazenamento disponível a cada 15 minutos. Sempre que o espaço de armazenamento for menor que o valor especificado, o Agente do Arcserve UDP (Linux) executará o script *backup_storage_alert.sh.* É possível configurar o script *backup_storage_alert.sh* para executar qualquer tarefa quando o espaço de armazenamento de backup for menor.

Exemplo 1: é possível configurar o script para enviar automaticamente um alerta por email para lembrá-lo de que o espaço de armazenamento está diminuindo.

Exemplo 2: é possível configurar o script para excluir automaticamente alguns dados do espaço de armazenamento de backup quando o espaço de armazenamento for menor que o valor especificado.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie o script *backup_storage_alert.sh* usando as seguintes variáveis:

   backupstoragename

   Define o nome do local de armazenamento de backup. Por exemplo: NFS ou CIFS.

   freesize

   Define o espaço livre disponível no local de armazenamento de backup.
3. Coloque o script no seguinte local:

   ```
   /opt/Arcserve/d2dserver/usr/alert/backup_storage_
   alert.sh
   ```

   O script backup_storage_alert.sh é criado.

Detectar nós usando um script

O Agente do Arcserve UDP (Linux) permite executar um script que detecta nós na sua rede. É possível gravar um script para detectar nós na rede e, em seguida, colocar o script na pasta de *detecção*.

É possível definir a configuração de detecção de nós na interface da web e definir a frequência de execução do script. No script, é possível especificar os utilitários para detectar nós na rede. Depois que o script detectar um nó, use o comando *d2dnode* para adicionar esse nó ao Agente do Arcserve UDP (Linux). Há um log de atividades sempre que o script é executado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Caso deseje imprimir algo no Log de atividades a respeito de seu script de detecção de nós, é possível usar a variável de ambiente especial a seguir:

```
echo "print something into activity log" > "$D2D_DISCOVER_
OUTPUT"
```

Um script de exemplo é colocado na pasta de *detecção* no local a seguir, o qual pode detectar os nós Linux em uma sub-rede.

```
/opt/Arcserve/d2dserver/examples/discovery
```

É possível copiar o script de amostra para o local a seguir e modificar esse script de acordo com sua necessidade:

/opt/Arcserve/d2dserver/usr/discovery

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um script de detecção de nós e coloque o script na pasta de *detecção* no seguinte local:

   ```
   /opt/Arcserve/d2dserver/usr/discovery
   ```

3. Forneça a permissão de execução necessária para o arquivo de script.
4. Efetue logon na interface da web do .
5. Defina as configurações de detecção de nós no menu Nó para executar seu script.
6. Clique em Log de atividades e verifique se o script é executado.

   O Log de atividades exibe uma lista de todos os nós detectados.

   Os nós são detectados com êxito usando o script.

Criar os scripts para fazer backup do banco de dados Oracle

É possível criar scripts que se usa para fazer backup do banco de dados Oracle. Não é necessário interromper o banco de dados para executar um backup. Verifique se o banco de dados está no modo de log de arquivo. Se ele não estiver no modo de log de arquivo, altere o banco de dados para o modo de log de arquivo antes de fazer backup do banco de dados. Crie os dois scripts seguintes para fazer backup do banco de dados Oracle:

- **pre-db-backup-mode.sh** - Esse script prepara e mantém todo o banco de dados no modo de backup.
- **post-db-backup-mode.sh** – Esse script remove o banco de dados do modo de backup.

É possível especificar que os scripts sejam executados nos nós do banco de dados Oracle nas Configurações de scripts anteriores e posteriores do Assistente de backup.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie o script *pre-db-backup-mode.sh* usando o seguinte código:

```
#!/bin/bash

orauser="oracle"

="orasid orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

connect / as sysdba

alter database begin backup;

exit;

EOF

BOF
```

Observação: especifique o valor das variáveis *orauser* e *orasid* conforme definido no banco de dados Oracle.

3. Crie o script *post-db-backup-mode.sh* usando o seguinte código:

```
#!/bin/bash

orauser="oracle"

="orasid orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

connect / as sysdba

alter database end backup;

exit;

EOF

BOF
```

   Observação: especifique o valor das variáveis *orauser* e *orasid* conforme definido no banco de dados Oracle.

4. Forneça a permissão de execução para os dois scripts.
5. Coloque ambos os scripts no seguinte local:

```
/opt/Arcserve/d2dserver/usr/prepost/
```

6. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
7. Abra o Assistente de backup e navegue até à guia Avançado.
8. Na opção Configurações de scripts anteriores e posteriores, selecione o arquivo de script *pre-db-backup-mode.sh* na lista suspensa "Antes que o instantâneo seja tirado".
9. Na opção Configurações de scripts anteriores e posteriores, selecione o arquivo de script *post-db-backup-mode.sh* na lista suspensa "Depois o instantâneo é tirado".
10. Envie a tarefa de backup.

    A tarefa de backup será enviada.

    Os scripts são criados para fazer backup do banco de dados Oracle.

    Observação: o Agente do Arcserve UDP (Linux) oferece suporte a instantâneos de nível de volume. Para garantir a consistência dos dados, todos os arquivos de dados do banco de dados devem estar em um volume.

Para restaurar o banco de dados Oracle, consulte Como restaurar um banco de dados Oracle usando o Agente do Arcserve UDP (Linux).

Criar os scripts para fazer backup do banco de dados MySQL

É possível criar scripts que se usa para fazer backup do banco de dados MySQL. Não é necessário interromper o banco de dados para executar um backup. Crie os dois scripts seguintes para fazer backup do banco de dados MySQL:

- **pre-db-backup-mode.sh** - Esse script fecha todas as tabelas abertas e bloqueia todas as tabelas de todos os bancos de dados com um bloqueio de leitura global.
- **post-db-backup-mode.sh** - Esse script libera todos os bloqueios.

Você pode especificar que os scripts sejam executados nos nós do banco de dados MySQL nas Configurações de scripts anteriores e posteriores do Assistente de backup.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie o script *pre-db-backup-mode.sh* usando o seguinte código:

```
#!/bin/bash#

dbuser=root

dbpwd=rootpwd

lock_mysqldb(){

(

  echo "flush tables with read lock;"

  sleep 5

) | mysql -u$dbuser -p$dbpwd ${ARGUMENTS} }

}

lock_mysqldb &

PID="/tmp/mysql-plock.$!"

touch ${PID}
```

Observação: especifique o valor das variáveis *dbuser* e *dbpwd* conforme definido no banco de dados MySQL.

3. Crie o script *post-db-backup-mode.sh* usando o seguinte código:

```
#!/bin/bash

killcids(){

pid="$1"

cids=`ps -ef|grep ${pid}|awk '{if('$pid'==$3){print $2}}'`

para cid em ${cids}

do

        echo ${cid}

        kill -TERM ${cid}

done

echo -e "\n"

}

mysql_lock_pid=`ls /tmp/mysql-plock.* | awk -F . '{print
$2}'`

[ "$mysql_lock_pid" != "" ] && killcids ${mysql_lock_pid}

rm -fr /tmp/mysql-plock.*
```

4. Forneça a permissão de execução para os dois scripts.
5. Coloque ambos os scripts no seguinte local:

   ```
   /opt/Arcserve/d2dserver/usr/prepost/
   ```

6. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
7. Abra o Assistente de backup e navegue até à guia Avançado.
8. Na opção Configurações de scripts anteriores e posteriores, selecione o arquivo de script *pre-db-backup-mode.sh* na lista suspensa "Antes que o instantâneo seja tirado".
9. Na opção Configurações de scripts anteriores e posteriores, selecione o arquivo de script *post-db-backup-mode.sh* na lista suspensa "Depois o instantâneo é tirado".
10. Envie a tarefa de backup.

    A tarefa de backup será enviada.

    Os scripts são criados para fazer backup do banco de dados MySQL.

Observação: o Agente do Arcserve UDP (Linux) oferece suporte a instantâneos de nível de volume. Para garantir a consistência dos dados, todos os arquivos de dados do banco de dados devem estar em um volume.

Execute uma BMR (Bare Metal Recovery - Recuperação Bare Metal) do servidor do MySQL

Uma Recuperação bare metal (BMR) restaura o sistema operacional e os aplicativos de software e recupera todos os dados incluídos no backup. A BMR é o processo de restauração de um sistema de computador do estado bare metal. Bare metal é um computador sem sistema operacional, drivers e aplicativos de software. Depois que a restauração for concluída, o computador de destino será reinicializado automaticamente no mesmo ambiente operacional que o nó de origem do backup e todos os dados serão restaurados.

É possível executar uma BMR usando o endereço IP ou o endereço MAC (Media Access Control – Controle de Acesso à Mídia) do computador de destino. Se você inicializar o computador de destino usando o Live CD do agente do Arcserve UDP (Linux), será possível obter o endereço IP do computador de destino.

Se o servidor do MySQL estiver danificado, é possível restaurar todo o servidor executando uma BMR.

Para restaurar um servidor do MySQL, siga estas etapas:

1. Efetue logon no console do servidor de backup Linux como usuário raiz.
2. Execute uma recuperação bare metal usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte o Como executar uma recuperação bare metal (BMR) para máquinas Linux.
3. Após a conclusão da tarefa de BMR, efetue logon no computador de destino e certifique-se de que o banco de dados esteja restaurado.

   O servidor do MySQL foi recuperado com êxito.

Executar a recuperação do banco de dados MySQL

Quando um banco de dados MySQL é perdido ou corrompido, é possível executar uma recuperação no nível do arquivo para restaurar o banco de dados específico.

Siga estas etapas:

1. Efetue logon no computador de destino como um usuário raiz.
2. Interrompa o serviço do MySQL

3. Para restaurar no local original:
    1. Exclua os arquivos e diretórios da pasta atual do banco de dados MySQL.
    2. Restaure a pasta do banco de dados do ponto de recuperação para a pasta do banco de dados MySQL
4. Inicie o serviço do MySQL.

   O banco de dados é recuperado com êxito.

Usar os scripts para fazer backup e restaurar o banco de dados PostgreSQL

Os seguintes scripts estão disponíveis para fazer backup do banco de dados PostgreSQL. Ao executar os scripts, não é necessário interromper o banco de dados para executar um backup.

- **postgresql_backup_pre.sh:** esse script coloca o banco de dados em modo de backup.
- **postgresql_snapshot_post.sh:** esse script remove o banco de dados do modo de backup.
- **postgresql_settings:** trata-se de um arquivo de configuração em que as variáveis do PostgreSQL talvez precisem ser atualizadas.
- **postgresql_backup_post.sh:** esse script atualiza o log sobre o status do backup.

Pré-requisitos

Antes de iniciar o backup, certifique-se de fazer o seguinte:

- O nível de WAL é definido como arquivo morto (ou hot_standby)
- archive_mode está definido como ativado
- archive_command deve ser definido para especificar o local do arquivo morto

Observação: para aplicar as configurações, reinicialize o servidor depois de ajustá-las no arquivo postgresql.conf.

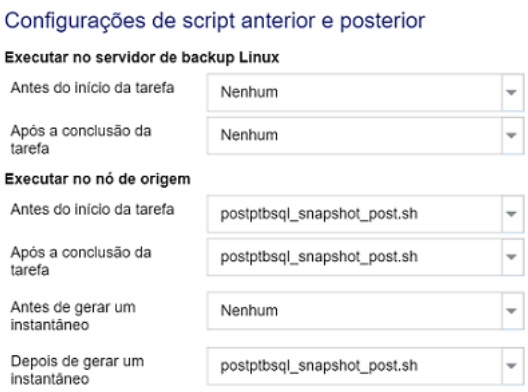
Os comandos a seguir ajudam a verificar o status do modo de arquivamento após a reinicialização:

- show archive_mode
- show archive_command
- show WAL level

Aplicar scripts

Siga estas etapas:

1. Extraia o LinuxPostgres.zip, que contém os seguintes quatro arquivos: postgresql_backup_pre.sh, postgresql_snapshot_post.sh, postgresql_settings, postgresql_backup_post.sh
2. Copie os arquivos do backup anterior/posterior/instantâneo para o seguinte caminho no servidor de backup do Linux: /opt/Arcserve/d2dserver/usr/prepost.
3. Copie postgresql_settings no caminho de origem /root/backup.
4. Certifique-se de verificar todos os valores definidos em postgresql_settings em relação às variáveis e fazer as modificações para todas as alterações necessárias de acordo com seu ambiente.
5. Configure o plano a partir do console do UDP e selecione o nó PostgreSQL como origem.



6. Confirme o status do backup. Para saber o status do backup do PostgreSQL, verifique o arquivo arcserve_postgresql_backup_${DATE}.log. Esse arquivo de log é criado no diretório definido pelo usuário. Para obter mais informações sobre como configurar o diretório, consulte o arquivo postgresql_settings.

Restaurar o banco de dados PostgreSQL

Siga estas etapas:

1. Interrompa o servidor de banco de dados.
2. Para restaurar para o local original, faça o seguinte:
    a. Exclua os arquivos e diretórios da pasta /data atual.
    b. Execute uma restauração de toda a pasta /data.
3. Depois de terminar de restaurar a pasta /data, exclua os arquivos das seguintes pastas:
    - pg_dynshmem/
    - pg_notify/
    - pg_serial/
    - pg_snapshots/
    - pg_stat_tmp/
    - pg_subtrans/
    - pg_internal.init
4. Acesse a pasta que está configurada para o arquivamento do WAL e faça o seguinte:
    a. Exclua os arquivos presentes no diretório pg_wal restaurado que contém as informações relacionadas às transações executadas durante o backup.
    b. Agora, copie os arquivos do local definido pelo usuário para a pasta pg_wal, para consistência de dados e recuperação pontual.
5. Inicie o servidor do banco de dados.

Restaure em um local diferente no mesmo servidor.

1. Interrompa o servidor de banco de dados.
2. Configure PGDATA em “new_data_directory_path” para executá-lo.
3. Inicialize o banco de dados recém-criado usando o comando “Initdb”.
4. Exclua os arquivos e diretórios da pasta /data atual.
5. Execute uma restauração de toda a pasta /data.
6. Depois de terminar de restaurar a pasta /data, exclua os arquivos das seguintes pastas:
    - pg_dynshmem/
    - pg_notify/

- pg_serial/
- pg_snapshots/
- pg_stat_tmp/
- pg_subtrans/
- pg_internal.init

7. Acesse a pasta que está configurada para o arquivamento do WAL e faça o seguinte:
   a. Exclua os arquivos presentes no diretório pg_wal restaurado que contém as informações relacionadas às transações executadas durante o backup.
   b. Agora, copie os arquivos do local definido pelo usuário para a pasta pg_wal, para consistência de dados e recuperação pontual.
8. Inicie o servidor do banco de dados.

   Observação: certifique-se de que a inicialização do banco de dados seja executada na sessão em que o PGDATA foi atualizado.

Limitações

Os scripts acima não ajudarão a executar backup se o banco de dados PostgreSQL estiver configurado com a porta não padrão. Os scripts trabalham somente com o número de porta padrão 5432.

Como alternativa, use as seguintes recomendações para modificar manualmente os scripts postgresql_backup_pre.sh e postgresql_snapshot_post.sh:

- postgresql_backup_pre.sh:

  Original: sudo -u ${USERNAME} -H -- psql -c "SELECT pg_start_backup('Arcserve UDP backup - ${DATE} $(timestamp)', true)" >> ${LOG} 2>&1

  Modificado: sudo -u ${USERNAME} -H -- psql -p 5432 -c "SELECT pg_start_backup('Arcserve UDP backup - ${DATE} $(timestamp)', true)" >> ${LOG} 2>&1

- postgresql_snapshot_post.sh:

  Original: sudo -u ${USERNAME} -H -- psql -c "SELECT pg_stop_backup()" >> ${LOG} 2>&1

  Modificado: sudo -u ${USERNAME} -H -- psql -p 5432 -c "SELECT pg_stop_backup()" >> ${LOG} 2>&1

Personalizar a programação de tarefas

O Agente do Arcserve UDP (Linux) permite que você defina sua própria programação usando um script para executar uma tarefa. Se você precisar executar uma tarefa periodicamente e não puder programar usando a interface do usuário da web, poderá criar um script para definir tal programação. Por exemplo, você deseja executar um backup às 22h00 no último sábado de cada mês. Não é possível definir essa programação usando a interface da web, mas é possível criar um script para defini-la.

É possível enviar uma tarefa de backup sem especificar nenhuma programação (usando a opção Nenhuma na página Avançado). Use o agendador Linux Cron para definir a programação personalizada e execute o comando *d2djob* para executar a tarefa.

Observação: o procedimento a seguir presume que você tenha enviado uma tarefa de backup sem especificar uma programação e que deseja executar um backup às 22h00 do último sábado de cada mês.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script, digite o comando a seguir para executar um backup às 22h00 do último sábado de cada mês:

```
#!/bin/bash#

LAST_SAT=$(cal | awk '$7!=""{t=$7} END {print t}')

TODAY=$(date +%d)

if [ "$LAST_SAT" = "$TODAY" ]; then

            source /opt/Arcserve/d2dserver/bin/setenv

            d2djob --run=your_job_name   --jobtype=your_job_
      type      #run your backup job here

fi
```

Observação: é necessário fornecer a permissão de execução necessária para o arquivo.

3. Navegue até à pasta crontab e adicione o seguinte comando na crontab de seu sistema (/etc /crontab):

```
00 22 * * Saturday root runjob.sh
```

O Cron executa o script runjob.sh às 22h00 todo sábado. No runjob.sh, ele primeiro verifica se hoje é o último sábado do mês. Se a resposta for sim, ele usa d2djob para executar a tarefa de backup.

A programação da tarefa é personalizada para executar um backup às 22h00 no último sábado de cada mês.

Executar uma tarefa em lotes de BMR

Se você deseja executar uma BMR em vários computadores e deseja instalar o mesmo ambiente operacional em todos os computadores, é possível executar uma BMR em lotes. Não é necessário criar uma tarefa para cada tarefa de BMR. Você pode economizar tempo e esforço, e pode reduzir o risco de qualquer erro ao configurar os computadores da BMR.

Observação: você deve ter um ponto de recuperação válido do computador de origem que deseja restaurar. Se não tiver um ponto de recuperação válido, primeiro você deverá fazer o backup do computador de origem e, em seguida, enviar uma tarefa de restauração.

Primeiro você define todas as configurações de BMR em uma tarefa de BMR modelo e, em seguida, altera o endereço (IP ou MAC), o nome do host e a configuração de rede do computador de destino usando o seguinte comando:

```
d2djob
```

Siga estas etapas:

1. Crie uma tarefa de BMR denominada BMR-MODELO e execute a tarefa para um computador dos seus vários computadores.

   Observação: você pode dar qualquer nome para a tarefa de BMR. Você deve fornecer o mesmo nome de tarefa no script da BMR em lotes.

2. Efetue logon no servidor de backup como usuário raiz.
3. Crie um script de BMR em lotes com base na tarefa BMR-MODELO para enviar automaticamente várias tarefas de BMR. Use o script a seguir para criar um script de BMR em lotes:

```
#!/bin/sh

prename=lab-server

serverList[0]="<MAC_Address>"

serverList[1]=" <MAC_Address>"

serverList[2]=" <MAC_Address>"

.

.

.

serverList[300]=" <MAC_Address>"
```

```
for((i=0;i<${#serverList[@]};i=i+1))

do

./d2djob --newrestore="BMR-MODELO" --target=${serverList[i]}
--hostname=$prename$i --network=dhcp

done
```

4. Execute o script de BMR em lote.

   O script é executado. Várias tarefas de BMR são criadas na interface do usuário.

   Um lote da tarefa BMR é executado.

Replicar e gerenciar sessões de backup

É possível criar um script para replicar as sessões de backup, de forma que seja possível recuperar dados quando os seus dados de backup originais estiverem corrompidos. As sessões de backup incluem todos os pontos de recuperação dos quais foram feitos backup. É possível proteger as sessões de backup replicando-as para um destino de replicação.

Depois de replicar as sessões de backup, você pode gerenciar o destino de replicação adicionando-o à interface do Agente do Arcserve UDP (Linux).

Replicar e gerenciar sessões de backup é um processo de três partes. Ele inclui as seguintes três partes:

- Replicar as sessões de backup para o destino de replicação
- Criar ou atualizar os arquivos de configuração dos pontos de recuperação para que os pontos possam ser gerenciados e exibidos na interface da web do Agente do Arcserve UDP (Linux)
- Adicionar o destino de replicação à interface da web do Agente do Arcserve UDP (Linux)

Replicar as sessões de backup

É possível aproveitar o recurso de Configurações de scripts anteriores e posteriores no Assistente de backup para replicar as sessões de backup no destino de replicação. É possível escolher qualquer opção, como FTP (File Transfer Protocol - Protocolo de Transferência de Arquivos), SCP (Secure Copy - Cópia Protegida) ou comando cp para replicar a sessão de backup.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um script anterior/posterior para replicar as sessões de backup.
3. Coloque o script no seguinte local:

   `/opt/Arcserve/d2dserver/usr/prepost`

4. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
5. Abra o Assistente de backup e vá até a guia Avançado.
6. Na opção Configurações de scripts anteriores e posteriores para Executar no servidor de backup, selecione o script de replicação na lista suspensa Após a conclusão da tarefa.
7. Envie a tarefa de backup.

   A sessão de backup é replicada para o destino de backup.

Criar ou atualizar os arquivos de configuração do ponto de recuperação

Depois de replicar as sessões de backup, crie e configure o arquivo de configuração dos pontos de recuperação. Esse arquivo é usado para identificar os pontos de recuperação quando você executa a operação de restauração pela interface do Agente do Arcserve UDP (Linux).

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá até o seguinte local:

   ```
   /opt/Arcserve/d2dserver/bin
   ```

3. Insira o comando a seguir para criar ou atualizar o arquivo de configuração dos pontos de recuperação:

   ```
   ./d2drp --storagepath=/backupdestination --node=node_name --session=session_name
   ```

   Se você fornecer apenas as informações de *--storagepath* e *--node*, o comando atualizará todas as sessões de backup do nó selecionado. Se você fornecer as informações de *--session*, o comando atualizará as informações da sessão específica.

   Observação: para obter mais informações sobre o comando d2drp, consulte *Entendendo os utilitários de script*.

   O arquivo de configuração dos pontos de recuperação será criado ou atualizado, dependendo do status do arquivo.

Adicionar o destino de replicação

Adicione o destino de replicação à interface do Agente do Arcserve UDP (Linux) para gerenciar o destino. Depois de adicionar o destino de replicação, será possível ver o espaço livre disponível naquele destino e gerenciar os dados de forma adequada.

Siga estas etapas:

1. Efetue logon no destino de replicação.
2. Crie um arquivo denominado Configurações e insira o código a seguir no arquivo Configurações:

   ```
   RecoverySetLimit=n
   ```

   n indica o número de conjuntos de recuperação que você deseja manter no destino de replicação.

3. Coloque o arquivo na pasta do nó do destino de replicação.

   Por exemplo, /destino_de_backup/nome_do_nó/Configurações

4. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
5. Adicione o destino de replicação a partir do menu Armazenamento de backup.

   O destino de replicação é adicionado à interface da web do Agente do Arcserve UDP (Linux).

   As sessões de backup são replicadas e gerenciadas com êxito.

Verificar se os pontos de recuperação são utilizáveis

O utilitário d2dverify ajuda a verificar se os pontos de recuperação de várias sessões de backup são utilizáveis. Normalmente, as tarefas de backup são executadas todos os dias e quando você tiver vários pontos de recuperação, pode não ter certeza de que os pontos de recuperação podem ser usados para recuperação de dados durante uma falha do sistema. Para evitar tais situações, é possível executar tarefas BMR periodicamente para verificar se os backups são utilizáveis. O utilitário d2dverify ajuda a automatizar a tarefa de verificar a usabilidade dos pontos de recuperação.

Após configurar os parâmetros necessários, o utilitário d2dverify envia a tarefa BMR e recupera os dados para a VM especificada. Em seguida, o d2dverify inicia a VM e executa um script para verificar se os aplicativos na VM funcionam corretamente. Também é possível criar uma programação para executar periodicamente o utilitário d2dverify usando utilitários do sistema, como o cron do Linux. Por exemplo, é possível executar o utilitário d2dverify após o último backup de um conjunto de recuperação. Neste caso, o d2dverify verifica todos os pontos de recuperação do conjunto de recuperação.

Observação: para obter mais informações sobre como agendar uma tarefa com o agendador cron do Linux, consulte Personalizar a programação de tarefas.

O utilitário d2dverify também pode ser usado nos seguintes cenários:

- É possível usar o utilitário d2dverify para migrar os backups de várias máquinas físicas para máquinas virtuais.
- Após a recuperação de um hipervisor, é possível usar o utilitário d2dverify para restaurar todas as VMs para o novo hipervisor.

Considere os pré-requisitos a seguir antes de usar o utilitário d2dverify:

- Identifique os nós de origem cujo backup você deseja verificar.
- Identifique o hipervisor no qual as VMs serão criadas.
- Crie VMs para cada nó que deseja verificar. Atribua o nome da VM no seguinte formato:

  `verify_<nome do nó>`

  Observação: não é necessário anexar discos rígidos virtuais para as VMs. Além disso, você não pode vincular rede virtual a essas VMs se você especificar os parâmetros "vm_network".

- Revisar os requisitos da rede

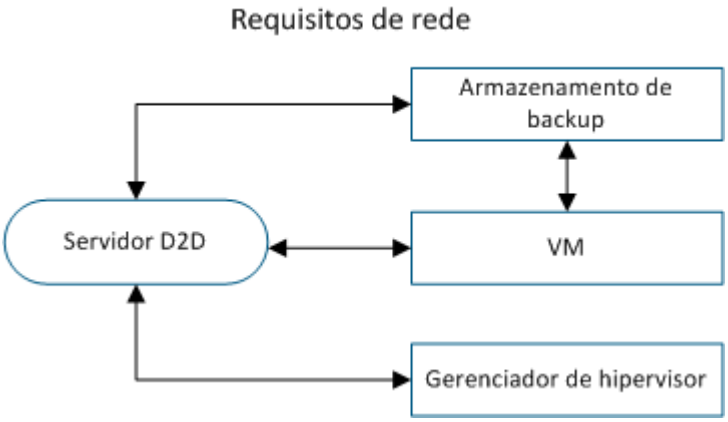
- Identifique uma rede na qual as VMs estarão conectadas.

  Observação: o utilitário d2dverify oferece suporte somente à rede de IP estático.

Importante: Se o banco de dados tiver informações sobre a conta do nó relacionadas a um usuário não raiz, o d2dverify irá redefinir a senha do usuário não raiz para 'CAd2d@2013 para a VM de destino.

Requisitos da rede:

Quando você usa o d2dverify, é recomendável manter as VMs de destino em uma rede virtual isolada para evitar conflitos com o ambiente de produção. Em tais casos, as VMs de destino devem estar conectadas ao servidor de backup e ao armazenamento de backup.



Suporte ao hipervisor:

O d2dverify depende do utilitário d2drestorevm para executar a restauração. O d2dverify oferece suporte às seguintes versões de hipervisor:

- XenServer 6.0 e posterior
- OVM 3.2

Argumentos:

--template

Identifica o modelo que inclui os parâmetros para executar o utilitário d2dverify.

--createtemplate

Cria um modelo vazio que inclui os parâmetros para executar o utilitário d2dverify.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie o modelo que é usado pelo utilitário d2dverify usando o seguinte comando:

   ```
   d2dverify --createtemplate=file_path
   ```

3. Abra o modelo e atualize os seguintes parâmetros:

   node_list

   Especifica uma lista de nós ou um critério de consulta que consulta informações no banco de dados do servidor de backup. Cada nó é separado por uma vírgula, como Nó1,Nó2,Nó3.

   Observação: se o número de porta SSH não for a porta padrão 22, o formato para especificar cada nó é: Nó1:nova_porta,Nó2:nova_porta,Nó3:nova_porta. O nome da VM é atribuído como verify_<nome do nó>, em que o nome do nó não inclui o número da porta.

   Exemplo: Nó1:222,Nó2:333,Nó4:333

   A lista a seguir é um exemplo de critérios de consulta:

   [node=prefix]

   Localiza o nome do nó que contém o prefixo definido.

   [desc=prefix]

   Localiza a descrição do nó que contém o prefixo definido.

   guest_ip_list =

   Especifica a lista de endereços IP que será aplicada a cada nó de destino, respectivamente. Cada endereço IP é separado por uma vírgula, como IP1,IP2,IP3. Se houver apenas um endereço IP disponível, mas vários nós no parâmetro node_list, o quarto segmento do endereço IP será aumentado em uma unidade para cada nó. O utilitário d2dverify verifica se um endereço IP foi usado. Se a resposta for sim, o endereço IP é ignorado.

   Por exemplo, se você tiver três nós, Nó 1, Nó 2 e Nó 3 e um endereço IP, xxx.xxx.xxx.xx6, o endereço IP é aplicado conforme mostrado na lista a seguir:

   Nó 1: xxx.xxx.xxx.xx6

   Nó 2: xxx.xxx.xxx.xx7

   Nó 3: xxx.xxx.xxx.xx8

   vm_type

   Especifica o tipo de hipervisor. São válidos os seguintes três tipos de hipervisor: xen ou ovm.

vm_server

Especifica o nome do host ou o endereço IP do gerenciador de hipervisor.

vm_svr_username

Especifica o nome de usuário do gerenciador de hipervisor.

vm_svr_password

Especifica a senha do gerenciador de hipervisor. A senha deve ser criptografada usando o utilitário --encrypt do d2dutil.

O comando a seguir é usado para criptografar a senha:

```
echo "password" | d2dutil --encrypt
```

vm_network

Especifica a rede virtual usada pela VM de destino. É recomendável especificar este parâmetro quando a VM de destino estiver conectada a várias redes virtuais.

guest_gateway

Especifica o gateway da rede usado pelo SO (Sistema Operacional) do hóspede da VM de destino.

guest_netmask

Especifica a máscara de rede que é usada pelo SO convidado da VM de destino.

guest_username

Especifica o nome de usuário utilizado para estabelecer uma conexão com a VM recuperada. A senha é redefinida como a senha especificada no parâmetro guest_password. O parâmetro guest_username é ignorado quando você usa o utilitário d2dverify para consultar informações no banco de dados do servidor de backup. Em tais casos, a senha de convidado da VM é redefinida para a senha do nó armazenada no banco de dados.

guest _password

Especifica a senha do parâmetro guest_username. A senha deve ser criptografada usando o utilitário --encrypt do d2dutil. O parâmetro guest_ password é ignorado quando você usa o utilitário d2dverify para consultar informações no banco de dados do servidor de backup.

storage_location

Especifica o caminho de rede do local de armazenamento de backup. Você não precisará especificar o local de armazenamento se os nós no parâmetro

node_list estiverem no banco de dados do servidor de backup. Se o local de armazenamento for um compartilhamento CIFS, use o seguinte formato para especificar o local:

```
//hostname/path
```

storage_username

Especifica o nome do usuário para acessar o local de armazenamento de backup. Esse parâmetro não é obrigatório para um compartilhamento de NFS.

Para um usuário de domínio do Windows, use o seguinte formato para especificar o local:

```
nome_do_domínio/nome do usuário
```

storage_password

Especifica a senha para acessar o local de armazenamento de backup. A senha deve ser criptografada usando o utilitário --encrypt do d2dutil. Esse parâmetro não é obrigatório para um compartilhamento de NFS.

recovery_point = last

Especifica a sessão que você deseja restaurar. Em geral, uma sessão de recuperação está no seguinte formato: S00000000X, em que X é um valor numérico. S00000000X é o nome da pasta dos pontos de recuperação. Se desejar restaurar a sessão mais recente, especifique a palavra-chave “last”.

encryption_password

Especifica a senha criptografada para o ponto de recuperação. A senha deve ser criptografada usando o utilitário --encrypt do d2dutil.

Script

Especifica o script que deseja executar. O script é executado no computador de destino após a recuperação com êxito. Se esse parâmetro não for fornecido, o utilitário d2dverify executa o comando ‘ls /proc’ no computador de destino.

email_to_address

Especifica o endereço de email dos destinatários que receberão relatórios por email. É possível especificar mais de um endereço de email, separados por vírgula.

email_subject

Especifica a linha de assunto do email.

report_format

Especifica o formato do relatório que você receberá por email. O formato pode ser de texto (.txt) ou html.

Padrão: html

node_not_in_db

Especifica os nós dos parâmetros node_list que não estão no banco de dados do servidor de backup. Você deve especificar os parâmetros relacionados a storage_*.

Valor: sim

stop_vm_after_recovery

Especifica que a VM de destino é interrompida após uma recuperação e verificação bem-sucedida. Os valores para esse parâmetro são yes e no.

Padrão: yes

4. Salve e feche o modelo.
5. Execute o utilitário d2dverify usando o seguinte comando:

   ```
   d2dverify --template=file_path
   ```

   Observação: o utilitário d2dverify falha se os nós no parâmetro node_list forem adicionados usando a chave pública/privada. Para resolver esse problema, defina a variável de ambiente 'export D2D_SSH_IGNORE_PWD=yes' no ambiente do shell em que você executa o utilitário d2dverify.

   A usabilidade de pontos de recuperação foi verificada com êxito.

Como gerenciar as configurações do servidor de backup

É possível executar as tarefas a seguir para gerenciar o servidor de backup:

- Configurar a duração para reter o histórico de tarefas e os logs de atividades
- Configurar a duração para reter os logs de depuração
- Alterar o número da porta SSH (Secure Shell) do servidor de backup

Execute as tarefas a seguir para gerenciar as configurações do servidor de backup:

- Verificar os pré-requisitos para gerenciar o servidor de backup
- Definir as configurações do histórico de tarefas e de retenção do log de atividades
- Definir as configurações de retenção do log de depuração
- Configurar a duração do tempo limite da IU
- Alterar o número da porta SSH do servidor de backup
- Gerenciar os conjuntos de recuperação
- Desativar os serviços BOOTPD e TFTPD
- Melhorar o desempenho da consulta do histórico de tarefas e log de atividades
- Ignorar verificação de cliente CIFS e NFS
- Ignorar validação de NFS e CIFS no servidor de backup Linux
- Configurar a pasta temporária padrão
- Configurar o caminho de instantâneo para o nó de backup
- Configurar as informações de conexão do servidor Hyper-V para a VM instantânea

Verificar os pré-requisitos para gerenciar o servidor de backup

Considere os pré-requisitos a seguir antes de gerenciar o servidor de backup:

- Você possui credenciais de logon raiz para o servidor de backup.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Definir as configurações do histórico de tarefas e de retenção do log de atividades

É possível configurar a duração para reter o histórico de tarefas e os logs de atividades. Se você deseja reter os logs de atividades e o histórico de tarefas por um período mais longo, é necessário configurar o arquivo do servidor.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Observação: se o arquivo não estiver presente, crie o arquivo server.cfg.
3. Adicione a seguinte linha ao arquivo server.cfg:

   ```
   job_history_activity_log_keep_day=<número de dias>
   ```

   Exemplo: para manter o histórico de tarefas e o log de atividades por 30 dias, digite a seguinte linha:

   ```
   job_history_activity_log_keep_day=30
   ```

   Observação: por padrão, o histórico de tarefas e os logs de atividade são retidos por 90 dias.

   O histórico de tarefas e o log de atividades são retidos durante o período especificado.

Definir as configurações de retenção do log de depuração

É possível configurar a duração para reter os logs de depuração. Se deseja reter os logs de atividades por um período mais longo, é necessário configurar o arquivo do servidor.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Observação: por padrão, o histórico de tarefas e os logs de atividade são retidos por 90 dias.

3. Adicione a seguinte linha ao arquivo server.cfg:

   ```
   d2d_log_keep_day=<número de dias>
   ```

   Exemplo: para reter o log de depuração por 30 dias, digite a seguinte linha:

   ```
   d2d_log_keep_day=30
   ```

   Observação: por padrão, os logs de depuração são retidos por 90 dias.

   O log de depuração do Agente do Arcserve UDP (Linux) é retido pelo período especificado.

Configurar a duração do tempo limite da IU

É possível configurar o arquivo de configuração webserver para que você seja desconectado da IU quando ela estiver inativa. Depois de configurar o arquivo, se não houver nenhuma atividade na IU durante o tempo especificado, você será desconectado automaticamente. É possível efetuar logon novamente e continuar sua atividade.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg a partir do seguinte local:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

   Observação: se o arquivo server.cfg não estiver presente, crie-o.

3. Adicione a seguinte linha ao arquivo server.cfg:

   `ui_timeout=<valor>`

   Exemplo:

   O valor deve estar em minutos. O limite máximo para o valor do tempo limite da IU é 60.

   `ui_timeout=40`

   O exemplo indica que, se o servidor de backup não detectar nenhuma atividade na interface do usuário por 40 minutos, ele efetuará o logoff do usuário.

4. Atualize o navegador da web para implementar as alterações.

   A duração do tempo limite da IU é configurada.

Alterar o número da porta SSH do servidor de backup

O servidor de backup usa a porta 22 padrão do SSH (Secure Shell) para se conectar aos nós. Se você deseja alterar a porta padrão para uma porta diferente, é possível configurar o arquivo server.env para especificar a nova porta.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.env.

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Observação:se o arquivo não estiver presente, crie o arquivo server.env.
3. Adicione a seguinte linha ao arquivo server.env e salve o arquivo:

   ```
   export D2D_SSH_PORT=new_port_number
   ```

   O número new_port_number deve ser um valor numérico.
4. Reinicie o servidor de backup.

   Depois de configurar o arquivo server.env, todas as tarefas, com exceção da tarefa de BMR, utilizam o novo número de porta para se conectar ao nó de destino. A tarefa de BMR usa a porta padrão.

   O número da porta do SSH do servidor de backup é alterado com êxito.

Gerenciar os conjuntos de recuperação

Gerenciar os conjuntos de recuperação inclui excluir os conjuntos de recuperação. Você deve gerenciar os conjuntos de recuperação regularmente para que possa ter conhecimento do espaço livre disponível. É possível planejar o armazenamento dos conjuntos de recuperação apropriadamente. Existem duas formas de gerenciar os conjuntos de recuperação:

- **Método 1:** gerenciar usando um armazenamento de backup dedicado. Neste método, o armazenamento de backup gerencia os conjuntos de recuperação a cada 15 minutos. É possível gerenciar apenas os repositórios de backup que o servidor de backup pode acessar. Se você escolher o local de origem como o destino do backup, você tem que compartilhar a pasta local.
- **Método 2:** gerenciar usando uma tarefa de backup. Neste método, a tarefa de backup gerencia os conjuntos de recuperação. Esses conjuntos de recuperação são gerenciados após a conclusão da tarefa de backup. É possível gerenciar os conjuntos de recuperação que estão armazenados no local de origem.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg.

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Observação: se o arquivo não estiver presente, crie o arquivo server.cfg.
3. Adicione a seguinte linha ao arquivo server.cfg e salve o arquivo:

   ```
   manage_recoveryset_local=0 ou 1
   ```

   O valor 0 indica que o arquivo usa o método 1.

   O valor 1 indica que o arquivo usa o método 2.
4. Reinicie o servidor de backup.

   Esses conjuntos de recuperação são gerenciados na linha de comando do servidor de backup.

Desativar os serviços BOOTPD e TFTPD

É possível desativar os serviços BOOTPD e TFTPD se não precisar da função de BMR de PXE.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.env.

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Observação: se o arquivo server.env não existir, crie-o.
3. Adicione o seguinte parâmetro ao arquivo server.env e salve o arquivo:

   ```
   export D2D_DISABLE_PXE_SERVICE=yes
   ```
4. Reinicie o servidor de backup.

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

   Os serviços BOOTPD e TFTPD foram desativados com êxito.

Melhorar o desempenho da consulta do histórico de tarefas e log de atividades

Se você tiver um grande arquivo do banco de dados, consultar o histórico de tarefas e o log de atividades demora bastante. É possível melhorar o tempo de consulta do histórico de tarefas e do log de atividades com o uso de opções específicas, obtendo o resultado em um curto período de tempo.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Observação: se o arquivo não estiver presente, crie o arquivo server.cfg.
3. Adicione as seguintes linhas ao arquivo server.cfg:
   - Para melhorar o desempenho da consulta do histórico de tarefas, adicione a seguinte linha:

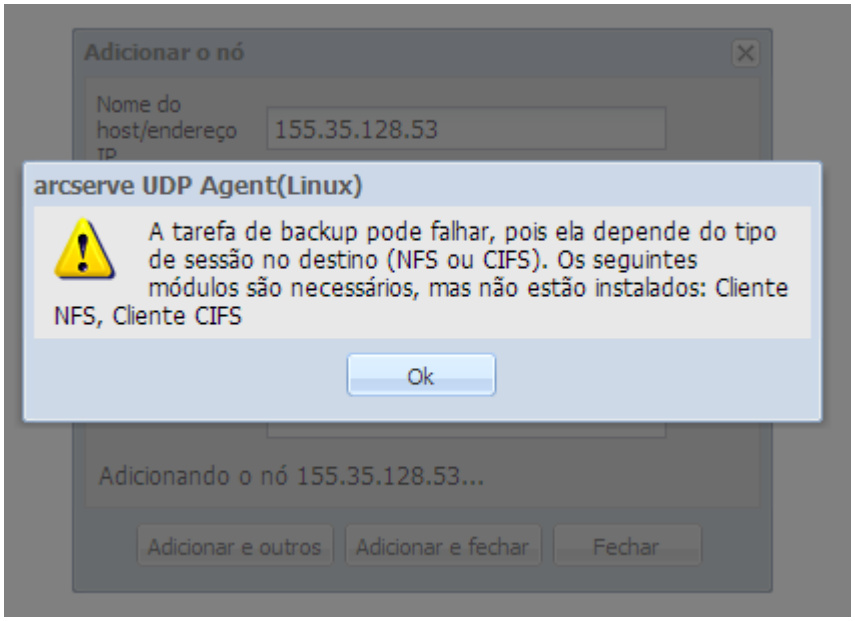
     ```
     skip_getting_job_history_count=true
     ```
   - Para melhorar o desempenho da consulta do log de atividades, adicione a seguinte linha:

     ```
     skip_getting_activity_log_count=true
     ```
4. Salve o arquivo server.cfg.

   O tempo de consulta do histórico de tarefas e do log de atividades foi aprimorado com êxito.

Ignorar a verificação dos módulos CIFS e NFS

Ao adicionar ou modificar um nó, o servidor de backup verifica os módulos CIFS e NFS no nó de destino. Se nenhum módulo estiver instalado, uma caixa de diálogo de aviso será exibida. É possível ocultar essa caixa de diálogo configurando o arquivo server.cfg.



Siga estas etapas:

1. Efetue logon no servidor de backup.
2. Abra o arquivo server.cfg:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

3. Adicione os parâmetros a seguir:

   `skip_client_check=nfs,cifs`

   Esse exemplo ignora a verificação dos módulos NFS e CIFS no nó de destino. Quando você fornece os dois módulos, a verificação é ignorada para ambos. Quando você fornece apenas um módulo, a verificação é ignorada apenas para esse módulo.

4. Salve o arquivo server.cfg.

   A verificação é ignorada para os módulos CIFS e NFS.

Ignorar validação de NFS e CIFS no servidor de backup Linux

Quando você adiciona ou modifica o armazenamento de backup, o servidor de backup valida se o CIFS ou o NFS está acessível no servidor de backup Linux. Se você quiser ignorar essa validação no servidor de backup Linux, poderá configurar o arquivo server.env.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Observação:se o arquivo não estiver presente, crie o arquivo server.env.
3. Adicione a seguinte linha ao arquivo server.env:

   ```
   export skip_validate_backup_storage_on_server=true
   ```
4. Reinicie o servidor de backup.

Configurar a pasta temporária padrão

Ao fazer backup de nós do Linux, a pasta **/tmp** padrão é usada para armazenar o binário necessário, dados de instantâneo temporários e os logs de depuração. A pasta /tmp deve ter espaço vazio suficiente e as permissões necessárias para executar os binários. Para alterar o caminho padrão em nós do Linux, é possível configurar o arquivo server.env e especificar os novos caminhos.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Observação: se o arquivo não estiver presente, crie o arquivo server.env.

3. Para configurar o caminho de execução do agente de nós do Linux, adicione a seguinte linha no arquivo server.env:

   ```
   export TARGET_BOOTSTRAP_DIR=<caminho>
   ```

   Exemplo: para implantar o agente do Linux sob o caminho **/d2dagent**, digite a seguinte linha:

   ```
   export TARGET_BOOTSTRAP_DIR=/d2dagent
   ```

   Observação: por padrão, o agente é implantado e executado sob a pasta /tmp.

4. Para configurar o caminho do repositório de dados de instantâneo temporário e o log de depuração do nó do Linux, adicione a seguinte linha ao arquivo server.env:

   ```
   export TARGET_WORK_DIR=<caminho>
   ```

   Exemplo: para configurar os logs de depuração e os dados de instantâneo temporários sob o caminho **/d2dagentlogs**, digite a seguinte linha:

   ```
   export TARGET_WORK_DIR=/d2dagentlogs
   ```

   Observação: por padrão, o agente é implantado e executado sob a pasta /tmp.

5. Reinicie o servidor de backup.

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

   A pasta temporária padrão é configurada.

Configurar o caminho de instantâneo para o nó de backup

Ao fazer backup de nós do Linux, a pasta **/tmp** padrão é usada para armazenar o arquivo de instantâneo do disco. A pasta **/tmp** deve ter espaço livre suficiente. Para alterar o caminho do instantâneo em nós do Linux, é possível configurar um arquivo específico de nó e definir o novo caminho.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá até a pasta do **nó**:

   `/opt/Arcserve/d2dserver/configfiles/node`

   Observação: se a pasta não existir, crie uma.

   A pasta **node** contém o arquivo <nome_do_nó>.cfg. Cada nó tem seu próprio arquivo .cfg.

3. Para configurar o caminho de instantâneo do nó do Linux, adicione a seguinte linha ao arquivo <nome_do_nó>.cfg específico:

   `target_snapshot_dir=<caminho>`

   Observação: se o arquivo <nome_do_nó>.cfg não existir, crie-o.

   Exemplo: se o nome do nó for **d2dbackupnode** e você quiser armazenar o instantâneo sob o caminho **/d2dsnapshot**, abra o seguinte arquivo cfg:

   `/opt/Arcserve/d2dserver/configfiles/node/d2dbackupnode.cfg`

   Adicione a linha a seguir:

   `target_snapshot_dir=/d2dsnapshot`

   A pasta do instantâneo é configurada no nó de destino.

Configurar as informações de conexão do servidor Hyper-V para a VM instantânea

Ao enviar tarefas de VM instantânea para nós do Linux, o servidor de Backup tenta detectar automaticamente o servidor Hyper-V. Mas se o processo falhar, é possível verificar se as informações de conexão do servidor Hyper-V usadas estão corretas.

A IVM (Instant Virtual Machine – Máquina Virtual Instantânea) do Linux oferece suporte ao Hyper-V com SMB 2.0 ou superior para evitar as vulnerabilidades do SMB 1.0.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá até a seguinte pasta do Hyper-V:

   `/opt/Arcserve/d2dserver/configfiles/hyperv`

   Observação: se a pasta não existir, crie uma. A pasta do Hyper-V contém o arquivo <upper_case_hyperv_server_name>.cfg. Cada servidor Hyper-V tem seu próprio arquivo cfg.

3. Para configurar as informações de conexão do Hyper-V, adicione as seguintes linhas no arquivo .cfg <node_name> específico:

   protocolo=<HTTP|HTTPS>

   porta=<number>

   Observação: se o arquivo <upper_case_hyperv_server_name>.cfg não existir, crie-o.

   Para o número da porta e protocolo, acesse o servidor Hyper-V de destino usando a seguinte linha de comando:

   winrm enumerate winrm/Config/Listener

   Por exemplo: o nome de destino do servidor Hyper-V é ivm-hyperv e o WinRM no servidor Hyper-V é configurado como HTTPS com escuta na porta 5986. Depois, abra o seguinte arquivo cfg:

   /opt/Arcserve/d2dserver/configfiles/hyperv/IVM-HYPERV.cfg

   Adicione as linhas a seguir:

   protocolo=HTTPS

   porta=5986

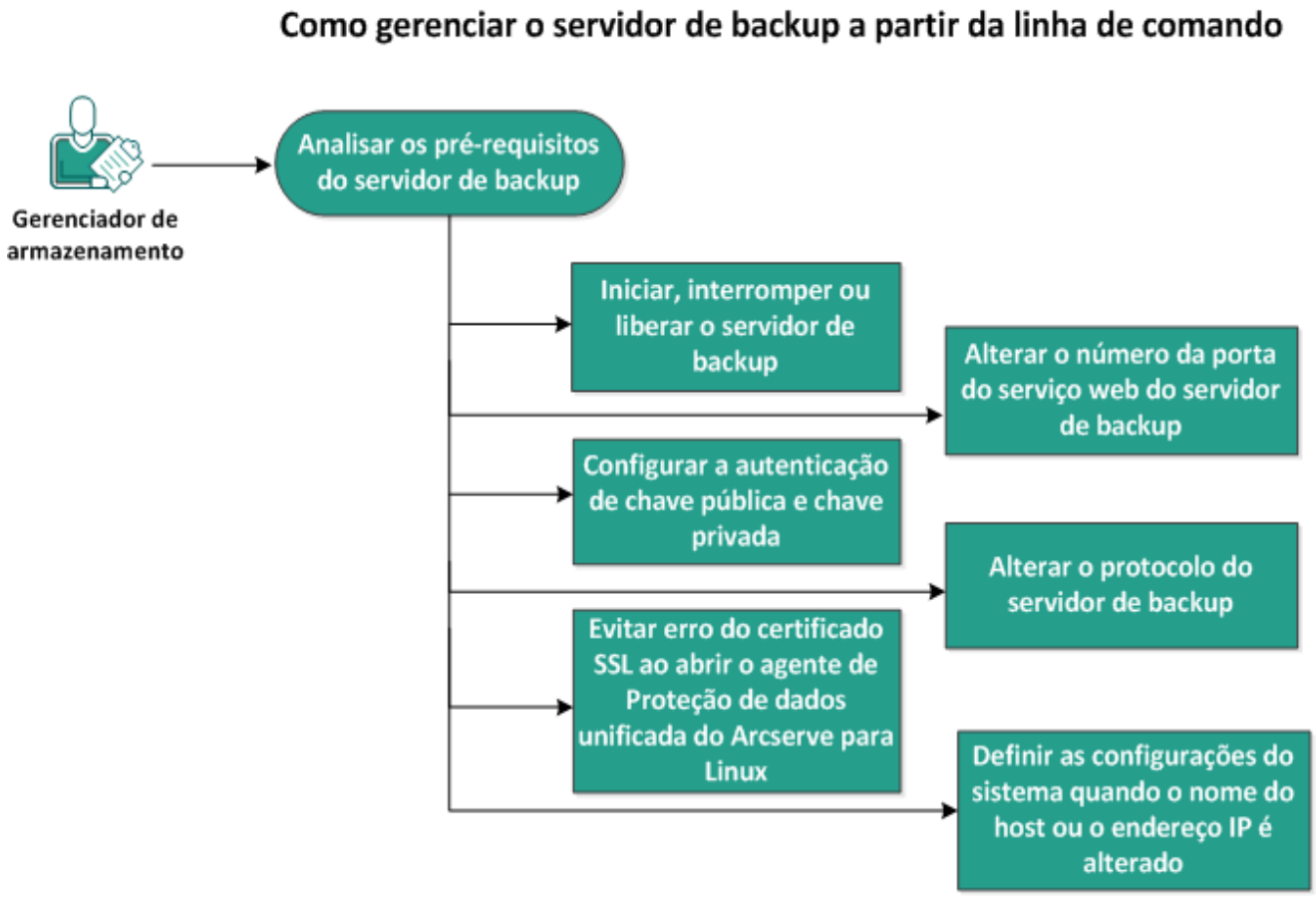
As informações de conexão do servidor Hyper-V são configuradas.

Como gerenciar o servidor de backup Linux a partir da linha de comando

O servidor de backup Linux executa todas as tarefas de processamento do Agente do Arcserve UDP (Linux). Para o funcionamento adequado do Agente do Arcserve UDP (Linux), você deve garantir que o servidor de backup esteja sempre em execução. É possível efetuar logon no servidor de backup e gerenciar o servidor usando alguns comandos.

Por exemplo, caso queira acessar a interface da web do Agente do Arcserve UDP (Linux), você deve garantir que o servidor web esteja em execução. É possível verificar o status de execução do servidor web no servidor de backup e garantir o funcionamento adequado do Agente do Arcserve UDP (Linux).

O diagrama a seguir exibe o processo para gerenciar o servidor de backup a partir da linha de comando:



Execute as tarefas a seguir para gerenciar o servidor de backup:

- Analisar os pré-requisitos do servidor de backup
- Iniciar, interromper ou liberar o servidor de backup

- Alterar o número da porta do serviço web do servidor de backup
- Configurar a autenticação de chave pública e chave privada
- Alterar o protocolo do servidor de backup
- Evitar o erro do certificado SSL ao abrir o Agente do Arcserve UDP (Linux)
- Definir as configurações do sistema quando o nome do host ou o endereço IP é alterado

Analisar os pré-requisitos do servidor de backup

Considere os pré-requisitos a seguir antes de gerenciar o servidor de backup:

- Você possui credenciais de logon raiz para o servidor de backup.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Iniciar, interromper ou liberar o servidor de backup

Gerencie o servidor de backup para saber o status de execução do servidor de backup. É possível verificar se o servidor de backup foi interrompido ou se ainda está em execução e, em seguida, gerenciar o servidor de forma adequada. O Agente do Arcserve UDP (Linux) oferece suporte às seguintes funções de linha de comando:

- Iniciar o servidor de backup
- Interromper o servidor de backup
- Liberar o servidor de backup

Siga estas etapas:

1. Navegue para a pasta bin usando o seguinte comando:

   ```
   # cd /opt/Arcserve/d2dserver/bin
   ```

   Você obtém acesso à pasta bin.

2. Na pasta bin, execute os comandos a seguir, dependendo da tarefa que você deseja executar no servidor:

   Observação: se algum comando não for bem-sucedido, uma mensagem de erro será exibida indicando o motivo.

   ```
   # ./d2dserver start
   ```

   Inicia o servidor de backup.

   Se você for bem-sucedido, uma mensagem será exibida informando que o servidor foi iniciado.

   ```
   # ./d2dserver stop
   ```

   Interrompe o servidor de backup.

   Se você for bem-sucedido, uma mensagem será exibida informando que o servidor foi interrompido.

   ```
   # ./d2dserver restart
   ```

   Reinicia o servidor de backup.

   Se você for bem-sucedido, uma mensagem será exibida informando que o servidor foi reiniciado.

   ```
   # ./d2dserver status
   ```

Exibe o status do servidor de backup.

```
# /opt/Arcserve/d2dserver/bin/d2dreg --release
```

Libera os demais servidores de backup que são gerenciados pelo servidor principal.

Por exemplo, se o servidor de backup A gerenciar dois outros servidores, o servidor de backup B e o servidor de backup C, quando você desinstalar o servidor de backup A, não será possível acessar o servidor de backup B nem o servidor de backup C. Você pode liberar o servidor de backup B e o servidor de backup C usando esse script e acessar esses servidores.

O servidor de backup foi gerenciado com sucesso a partir da linha de comando.

Alterar o número da porta do serviço web do servidor de backup

O Agente do Arcserve UDP (Linux) usa a porta 8014 por padrão. Se o número da porta 8014 já for usado por outro aplicativo, o Agente do Arcserve UDP (Linux) não funcionará corretamente. Nesse caso, você deve alterar o número de porta padrão do Agente do Arcserve UDP (Linux) para um número de porta diferente.

Siga estas etapas:

1. Abra o arquivo server.xml a partir do seguinte local:

   ```
   /opt/Arcserve/d2dserver/TOMCAT/conf/server.xml
   ```

2. Pesquise a sequência de caracteres a seguir no arquivo e altere o número de porta 8014 para o número de porta desejada:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" cli-
   entAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

3. Execute o comando a seguir para reiniciar o servidor de backup:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

   O número de porta padrão é alterado para o número de porta desejado.

Configurar a autenticação de chave pública e chave privada

A chave pública e a chave privada permitem que você se conecte com segurança a nós quando não fornecer a senha. Cada vez que o servidor de backup cria uma conexão SSH com os nós, o servidor de backup verificará a chave pública e a chave privada dos respectivos nós. Se as chaves não corresponderem, será exibida uma mensagem de erro.

Observação:

- Apenas os usuários que têm a permissão raiz têm suporte para usar a autenticação de chave pública e chave privada. Não é necessário ter o nome de usuário como raiz. Os usuários não raiz não têm suporte para usar a autenticação de chave pública e chave privada. Os usuários não raiz devem fornecer a autenticação de senha e nome de usuário.
- A autenticação de chave pública e chave privada será aplicada quando a senha não for fornecida. O nome de usuário ainda é necessário e deve corresponder ao proprietário da chave.
- Ao usar a autenticação sudo, consulte Como configurar a conta de usuário Sudo para nós do Linux para uma configuração específica.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Gere uma chave pública/privada usando o comando ssh-keygen a seguir:

   ```
   ssh-keygen -t rsa -f server
   ```

   Dois arquivos são gerados, especificamente, server.pub e servidor.
3. Copie o arquivo da chave pública server.pub para o seguinte local:

   ```
   /opt/Arcserve/d2dserver/configfiles/server_pub.key
   ```
4. Copie o arquivo da chave privada server para o seguinte local:

   ```
   /opt/Arcserve/d2dserver/configfiles/server_pri.key
   ```
5. (Opcional) Execute o comando a seguir caso você tenha fornecido a senha ao gerar as chaves pública e privada:

   ```
   echo "passphrase" | ./d2dutil --encrypt > /opt/Arc-
   serve/d2dserver/configfiles/key.pass
   ```

6. Altere a permissão do arquivo key.pass usando o seguinte comando:

   ```
   chmod 600 /opt/Arcserve/d2dserver/configfiles/key.pass
   ```

7. Efetue logon no nó de origem.
8. Copie o conteúdo do arquivo server_pub.key para o servidor de backup no seguinte local do nó:

   ```
   /<user_home>/.ssh/authorized_keys
   ```

   Exemplo: para um backup_admin, user_home é */home/backup_admin*

   Exemplo: /home/backup_admin/.ssh/authorized_keys

9. (Opcional) Execute o seguinte comando no nó se o SELinux bloquear a autenticação:

   ```
   restorecon /<user_home>/.ssh/authorized_keys
   ```

   A chave privada e a chave pública são configuradas com êxito. É possível conectar os nós de origem com a chave pública e a chave privada.

Alterar o protocolo do servidor de backup

O Agente do Arcserve UDP (Linux) é instalado com o protocolo https. É possível alterar o protocolo se você não quiser transferir dados com criptografia. É recomendável usar o https, pois todos os dados transferidos por https são criptografados. Os dados transferidos por http são texto sem formatação.

Siga estas etapas:

1. Abra o arquivo server.xml a partir do seguinte local:

   ```
   /opt/Arcserve/d2dserver/TOMCAT/conf/server.xml
   ```

2. Pesquise a sequência de caracteres a seguir no arquivo server.xml:

   ```
   <!--<Connector connectionTimeout="180000" port="8014" pro-
   tocol="HTTP/1.1"/>-->
   ```

3. Remova os caracteres **<!--** e **-->** conforme mostrado no exemplo a seguir:

   Exemplo: a sequência de caracteres a seguir é a saída desejada após a remoção dos caracteres **<!--** e **-->**:

   ```
   <Connector connectionTimeout="180000" port="8014" pro-
   tocol="HTTP/1.1"/>
   ```

4. Pesquise a sequência de caracteres a seguir no arquivo server.xml:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" cli-
   entAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

5. Adicione a sequência de caracteres **<!--** e **-->** conforme mostrado no exemplo a seguir:

   Exemplo: a sequência de caracteres a seguir é a saída desejada após a adição dos caracteres **<!--** e **-->**:

   ```
   <!--<Connector port="8014" protocol="HTTP/1.1" SSLE-
   nabled="true" maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore" keys-
   torePass="LinuxD2D"/>-->
   ```

6. Execute o comando a seguir para reiniciar o servidor de backup:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

O protocolo do servidor de backup é alterado de https para http.

Evitar o erro do certificado SSL ao abrir o Agente do Arcserve UDP (Linux)

Remova o certificado SSL personalizado para não receber o erro do certificado ao abrir a interface da web do Agente do Arcserve UDP (Linux). Após configurar o certificado SSL, você não receberá o erro de certificado novamente.

Siga estas etapas:

- Use o certificado gerado pelo Agente do Arcserve UDP (Linux) para o Firefox.

  1. Abra o Agente do Arcserve UDP (Linux) no Firefox.
  2. Clique em Compreendo os riscos e, em seguida, clique em Adicionar exceção.

     A caixa de diálogo Adicionar exceção de segurança é exibida.
  3. Clique em Exibir para verificar o certificado.

     A caixa de diálogo Visualizador de certificado é exibida.
  4. Verifique os detalhes do certificado e clique em Fechar.

     Não é necessário executar qualquer ação na caixa de diálogo Visualizador de certificado.
  5. Na caixa de diálogo Adicionar exceção de segurança, marque a caixa de seleção Armazenar permanentemente esta exceção.
  6. Clique em Confirmar exceção de segurança.

     O certificado é adicionado.

- Use o certificado gerado pelo Agente do Arcserve UDP (Linux) para o IE (Internet Explorer) ou Chrome.

  1. Abra o Agente do Arcserve UDP (Linux) no IE ou Chrome.
  2. Clique em Continuar neste site (não recomendado).

     A barra de endereços é exibida em vermelho e uma mensagem Erro de certificado aparece na barra de status de segurança.
  3. Clique em Erro de certificado.

     A caixa de diálogo Certificado não confiável é exibida.

4. Clique em Exibir certificados.

   A caixa de diálogo Certificado é aberta.

5. Na guia Geral, clique em Instalar certificado.

   A opção Certificate Import Wizards é exibida.

6. Clique em Avançar.
7. Na página Repositório de certificados, selecione Colocar todos os certificados no repositório a seguir e clique em Procurar.
8. Selecione Autoridades de certificação raiz confiáveis e clique em OK.

   A página Repositório de certificados do Assistente para importação de certificados é exibida.

9. Clique em Avançar e, em seguida, em Concluir.

   A caixa de diálogo Aviso de segurança é exibida.

10. Clique em Sim.
11. Reinicie o IE ou o Chrome.

    O certificado é adicionado.

    Observação: depois de adicionar o certificado, o navegador Chrome ainda irá mostrar o ícone de erro para o certificado SSL na barra de endereços. Este é um lembrete de que o certificado não é identificado pelas autoridades de certificação, contudo, ele é confiável segundo o Chrome, e todos os dados transferidos pela rede são criptografados.

- Execute as seguintes etapas para usar um certificado assinado:

  1. Use o certificado assinado por uma autoridade de certificação.
  2. Importe o certificado assinado usando o comando keytool.

     O certificado é adicionado.

O erro do certificado ssl é resolvido.

Definir as configurações do sistema quando o nome do host ou o endereço IP é alterado

Se alterar o nome do host ou o endereço IP do servidor de backup ou o nó cliente (nó de backup), será necessário definir as configurações do sistema. Defina as configurações do sistema para ajudar a garantir o seguinte:

- Para garantir uma boa comunicação entre o servidor central e o servidor integrante. Um servidor integrante é um servidor de backup gerenciado a partir do servidor de backup central. Para gerenciar o servidor integrante a partir da IU do servidor central, é necessário adicionar o servidor integrante na IU do servidor central.
- Para garantir que depois de alterar o nome do host ou o endereço IP do nó cliente seja possível fazer backup do nó cliente sem nenhum erro.

Quando o nome do host do servidor de backup central é alterado

Quando você altera o nome do host do servidor de backup central, é preciso configurar o servidor para poder usar o Agente do Arcserve UDP (Linux) sem problemas.

Siga estas etapas:

1. Efetue logon no servidor de backup central como um usuário raiz.
2. Para atualizar o nome do host e as informações de licença, digite os seguintes comandos:

   ```
   source /opt/Arcserve/d2dserver/bin/setenv
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2d-server/data/ARCserveLinuxD2D.db "update D2DServer set Name='New_Hostname' where IsLocal=1"
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2d-server/data/License.db "update LicensedMachine set ServerName ='New_Hostname' where ServerName ='Old_Hostname'"
   ```

3. Renomeie o arquivo de keystore:

   ```
   mv /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore.old
   ```

4. Crie um arquivo de keystore usando o seguinte comando Java keytool.

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass <YOUR_VALUE> -storepass <YOUR_VALUE> -keystore
   ```

```
/opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore -vali-
dity 3600 -dname "CN=<New Hostname>"
```

Observação: atualize o campo SEU_VALOR de acordo com sua necessidade. Geralmente, o valor é a senha.

Exemplo:

```
keytool -genkey -alias tomcat -keyalg DSA -keypass LinuxD2D
-storepass LinuxD2D -keystore /opt/Arc-
serve/d2dserver/TOMCAT/conf/server.keystore -validity 3600 -
dname "CN=New Hostname"
```

5. Abra o arquivo de configuração do TOMCAT server.xml e altere o valor de keystoreFile e de keystorePass de acordo com o arquivo de keystore que acabou de criar:

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" cli-
entAuth="false" sslProtocol="TLS" keys-
toreFile="${catalina.home}/conf/server.keystore"
keystorePass="SEU_VALOR"/>
```

Exemplo:

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" cli-
entAuth="false" sslProtocol="TLS" keys-
toreFile="${catalina.home}/conf/server.keystore"
keystorePass="LinuxD2D"/>
```

6. Reinicie o Servidor de backup central.

```
/opt/Arcserve/d2dserver/bin/d2dserver restart
```

O servidor de backup central é configurado.

Quando o nome do host ou o endereço IP do servidor integrante é alterado

Ao alterar o nome do host ou o endereço IP do servidor de backup integrante, configure o servidor integrante para gerenciá-lo a partir do servidor central. Se você não configurar o servidor integrante, ocorrerá um erro ao tentar gerenciá-lo a partir do servidor central. Um servidor integrante é um servidor que foi adicionado à interface da web do servidor de backup central.

Siga estas etapas:

1. Efetue logon no servidor de backup integrante como um usuário raiz:
2. Para alterar o nome do host, digite os seguintes comandos:

```
source /opt/Arcserve/d2dserver/bin/setenv

/opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2d-
server/data/ARCserveLinuxD2D.db "update D2DServer set
Name='New_Hostname' where IsLocal=1"
```

3. Renomeie o arquivo de keystore:

```
mv /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore
/opt/Arcserve/d2dserver/TOMCAT/conf/

server.keystore.old
```

4. Crie um arquivo de keystore usando o seguinte comando Java keytool.

```
keytool -genkey -alias tomcat -keyalg DSA -keypass LinuxD2D
-storepass LinuxD2D -keystore /opt/Arcserve/d2d-
server/TOMCAT/conf/server.keystore -validity 3600 -dname
"CN=New Hostname"
```

Observação: atualize o campo SEU_VALOR de acordo com sua necessidade. Geralmente, o valor é a senha.

Exemplo:

```
keytool -genkey -alias tomcat -keyalg DSA -keypass LinuxD2D
-storepass LinuxD2D -keystore /opt/Arc-
serve/d2dserver/TOMCAT/conf/server.keystore -validity 3600 -
dname "CN=New Hostname"
```

5. Abra o arquivo de configuração do TOMCAT server.xml e altere o valor de keystoreFile e de keystorePass de acordo com o arquivo de keystore.

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" cli-
entAuth="false" sslProtocol="TLS" keys-
toreFile="${catalina.home}/conf/server.keystore"
keystorePass="SEU_VALOR"/>
```

Exemplo:

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" cli-
entAuth="false" sslProtocol="TLS" keys-
toreFile="${catalina.home}/conf/server.keystore"
keystorePass="LinuxD2D"/>
```

6. Reinicie o servidor de backup integrante.

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

7. Efetue logon na interface da web central do Arcserve UDP para Linux.
8. A partir do painel Servidores de backup, selecione o servidor do nome do host antigo.
9. No menu Servidor de backup, clique em Excluir.
10. Na caixa de diálogo Excluir, clique em OK.

    O servidor do nome do host antigo é excluído.

11. No menu Servidor de backup, clique em Adicionar.

    A caixa de diálogo Adicionar servidor é aberta.

12. Digite os detalhes do novo nome do host na caixa de diálogo e clique em OK.

    A caixa de diálogo Adicionar servidor é fechada e o servidor integrante com o novo nome do host é adicionado à IU.

13. Efetue logon no servidor de backup central que gerencia o servidor de backup integrante.
14. Para atualizar as informações de licença, digite os seguintes comandos:

    ```
    source /opt/Arcserve/d2dserver/bin/setenv
    ```

    ```
    /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2d-
    server/data/License.db "update LicensedMachine set Ser-
    verName ='New_Hostname' where ServerName ='Old_Hostname'"
    ```

    O servidor de backup integrante é configurado.

Quando o nome do host ou o endereço IP do nó cliente é alterado

Se você alterar o nome do host ou o endereço IP de um nó, é possível configurar o nome do host ou o endereço IP nas configurações do sistema, de modo que você possa fazer backup desse nó sem erros.

Siga estas etapas:

1. Efetue logon no destino do backup.
2. Localize a pasta denominada **Old_Hostname** no destino do backup deste nó e mude seu nome para **New_Hostname**.

   Por exemplo, considere que o nome do host antigo do nó 1 seja First_Node. O destino do backup para o nó 1 é //Backup_Destination/LinuxBackup. Depois de realizado o primeiro backup com êxito, uma pasta chamada First_Node é criada em

//Backup_Destination/LinuxBackup. Agora, você modificou o nome do host antigo para Second_Node. Localize a pasta First_Node em //Backup_Destination/LinuxBackup e mude seu nome para Second_Node.

3. Efetue logon no servidor de backup como usuário raiz.
4. Para atualizar o nome do host, digite os seguintes comandos:

   ```
   source /opt/Arcserve/d2dserver/bin/setenv
   ```

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=Backup Destination --node=New_Hostname
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db "update TargetMachine set Name='New_Hostname' where Name='Old_Hostname'"
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db "update JobQueue set TargetName='New_Hostname' where JobType in (1,3,4,5) and TargetName='Old_Hostname'"
   ```

   Observação: se você usar o compartilhamento de NFS ou CIFS como o destino do backup, você deve montá-lo no Compartilhamento local.

   Exemplo: se o ponto de montagem é /mnt/backup_destination.

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=<mount point> --node=New_Hostname
   ```

   Observação: se você usar o Compartilhamento local, o comando é:

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=<local path> --node=New_Hostname
   ```

5. Efetue logon no servidor de backup central como um usuário raiz.
6. Para atualizar as informações de licença, digite o seguinte comando:

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/License.db "update LicensedMachine set MachineName ='New_Hostname' where MachineName ='Old_Hostname'"
   ```

   O nome do host é configurado para a realização do backup sem erros.

Quando a VM do LBS é clonada em um ambiente virtual

Quando a VM do LBS é clonada em um ambiente virtual, ela contém a mesma UUID que o modelo clonado. Portanto, é necessário gerar a UUID novamente.

Siga estas etapas:

1. Efetue logon no servidor de backup Linux como usuário raiz.
2. Abra o prompt sqlite.

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arc-
   serve/d2dserver/data/ARCserveLinuxD2D.db
   ```

3. Obtenha a UUID do banco de dados sqlite.

   ```
   sqlite> selecione uuid a partir de D2DServer;

   702ab046-3b70-493d-a2e2-ef3ff3b4dc52
   ```

4. Exclua a UUID existente do banco de dados sqlite.

   ```
   sqlite> exclua a partir de D2DServer, com UUID="702ab046-
   3b70-493d-a2e2-ef3ff3b4dc52";
   ```

5. Reinicie os serviços UDP para gerar uma nova UUID.

   ```
   opt/Arcserve/d2dserver/bin # ./d2dserver restart
   ```

Como adicionar um usuário ao console do servidor de backup Linux usando a linha de comando

Com o agente do Arcserve UDP para Linux, usando a linha de comando, você pode criar um usuário que pode agir como substituto do usuário raiz no servidor Linux. É possível usar a linha de comando d2duser para adicionar um usuário desse tipo quando o usuário raiz está desativado.

O usuário raiz pode ser desativado por vários motivos. Por exemplo, quando você cria a máquina virtual no AWS EC2, o usuário raiz é desativado por padrão.

- Verificar os pré-requisitos
- Adicionar um usuário ao console do servidor de backup Linux usando a linha de comando

Verificar os pré-requisitos

Considere o seguinte pré-requisito ou ponto antes de adicionar o usuário:

- Você possui credenciais de logon raiz para o servidor de backup.
- Só o usuário raiz pode executar a linha de comando: d2duser.

Adicionar um usuário ao console do servidor de backup Linux usando a linha de comando

É possível usar a linha de comando d2duser para adicionar um usuário que pode agir como substituto do usuário raiz, quando necessário.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá para /opt/Arcserve/d2dserver/configfiles e abra o arquivo server.cfg.

   Observação: caso não exista um arquivo com esse nome, crie-o e adicione o seguinte conteúdo a ele:

   ui_login_use_udp_user= true|false

   Permite criar o usuário que age como o usuário padrão na ausência do usuário raiz quando você efetua logon no servidor. É possível selecionar **true** para essa opção.

   ui_login_user_password_min_length = 6

   Permite decidir o comprimento mínimo de senha. É possível modificar o valor padrão (6), se necessário.

   login_failure_time_to_lock_user = 9

   Permite decidir após quantas falhas consecutivas de logon a conta do usuário é bloqueada. É possível modificar o valor padrão (9), se necessário.
3. Vá para */opt/Arcserve/d2dserver/bin* e localize a linha de comando d2duser.
4. Digite /d2duser para exibir o uso dessa linha de comando:

   ```
   d2duser --action=<add|delete|lock|unlock|passwd> --user-
   name=<username>
   ```

5. Digite os seguintes detalhes na linha de comando d2duser:

   d2duser --action=add --username=arcserve

   Permite adicionar um usuário com o nome arcserve. Quando você pressiona Enter, é solicitada uma senha, a qual deve ser digitada uma segunda vez para ser confirmada.

   d2duser --action=delete --username=arcserve

   Permite excluir o usuário arcserve.

   d2duser --action=lock --username=arcserve

   Permite bloquear o usuário arcserve.

d2duser --action=unlock --username=arcserve

Permite desbloquear o usuário arcserve.

d2duser --action=passwd --username=arcserve

Permite alterar a senha do usuário arcserve.

d2duser --action=list

Permite exibir a lista de todos os usuários.

6. No navegador, abra a página do console do servidor de backup Linux.
7. Verifique se o usuário padrão exibido é aquele que você acaba de adicionar.
8. Efetue logon usando o nome de usuário e a senha definidos.

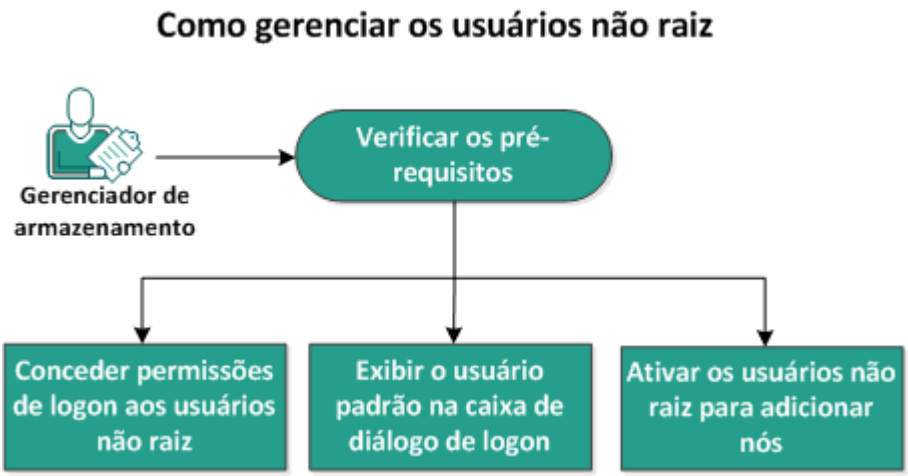
   O logon com êxito confirma que o usuário foi criado.

Como gerenciar os usuários não raiz

É possível gerenciar todos os usuários que não são raiz e acessam o Agente do Arcserve UDP (Linux) e definir as permissões para eles a fim de limitar o nível de acesso ao Agente do Arcserve UDP (Linux). É possível gerenciar os usuários não raiz modificando o arquivo de configuração webserver (arquivo server.cfg).

Observação: se o nó de origem do backup for configurado com pam_volante use a opção "usar_uid" para configurar pam_wheel. Para obter mais informações sobre pam_wheel, consulte a página principal de pam_wheel.

O diagrama a seguir exibe o processo para gerenciar os usuários não raiz:



Execute essas tarefas para gerenciar os usuários não raiz:

- Verificar os pré-requisitos
- Conceder permissões de logon aos usuários não raiz
- Exibir o usuário padrão na caixa de diálogo de logon
- Ativar os usuários não raiz para adicionar nós

Verificar os pré-requisitos

Considere os pré-requisitos a seguir antes de gerenciar os usuários não raiz:

- Você possui credenciais de logon raiz para o servidor de backup.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Conceder permissões de logon aos usuários não raiz

Um usuário raiz pode conceder permissões a usuários não raiz para efetuar logon no servidor de backup. Se usuários que não são raiz obtiverem permissão para efetuar logon no Servidor de backup, eles poderão usar o Agente do Arcserve UDP (Linux) para executar todas as tarefas de recuperação e proteção de dados.

Observação: para conceder permissões de logon aos usuários não raiz, conecte-se ao servidor de backup como usuário raiz usando a conexão SSH.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg a partir do seguinte local:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Observação: se o arquivo server.cfg não estiver presente, crie-o.

3. Adicione o seguinte código ao arquivo server.cfg:

   ```
   allow_login_users=user1 user2
   ```

   Observação: use espaços em branco para distinguir vários usuários.

   O código é adicionado.

4. Verifique se o usuário não raiz pode se conectar ao servidor de backup usando a conexão SSH.

   A permissão de logon é concedida aos usuários não raiz para acessar o servidor de backup.

Exibir o usuário padrão na caixa de diálogo de logon

É possível gerenciar seus usuários e alterar o nome que é exibido na caixa de diálogo de logon do Agente do Arcserve UDP (Linux). O usuário padrão que é exibido na caixa de diálogo de logon é o raiz. Se você não tiver usuários raiz acessando o produto, é possível alterar o nome padrão para o nome de qualquer usuário não raiz. Para fazer isso, modifique o arquivo server.cfg que está localizado no servidor de backup.

Observação: para modificar o arquivo server.cfg, conecte-se ao servidor de backup como usuário raiz usando a conexão SSH.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg a partir do seguinte local:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

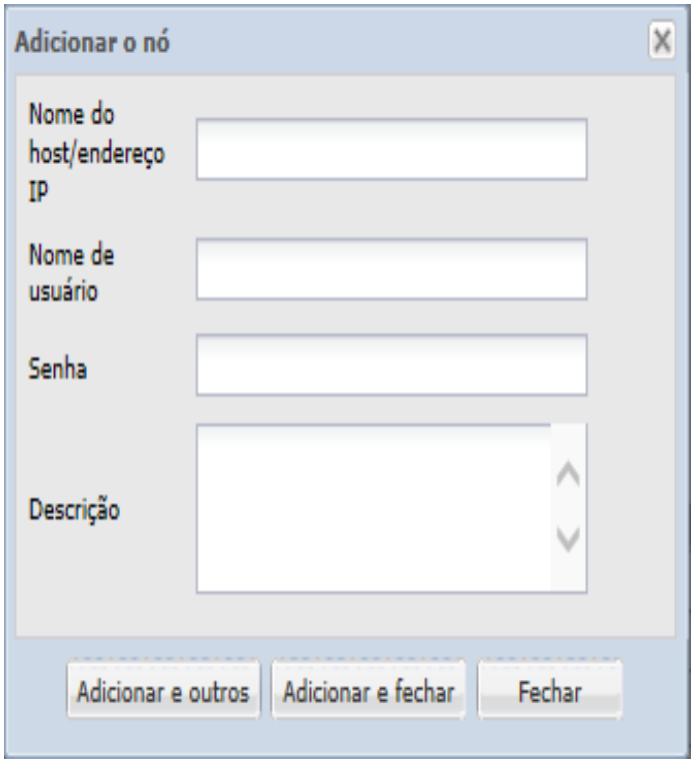
   Observação: se o arquivo server.cfg não estiver presente, crie-o.
3. Adicione o seguinte código ao arquivo server.cfg: show_default_user_when_login=false|true
4. Efetue logon na interface da web do Agente do Arcserve UDP (Linux).
   - Se você adicionou o comando *allow_login_users*, a caixa de diálogo de logon exibe o primeiro usuário adicionado ao comando *allow_login_users*.
   - Se você não adicionou o comando *allow_login_users*, a caixa de diálogo de logon exibe o usuário raiz.

   O usuário padrão é exibido na caixa de diálogo de logon do Agente do Arcserve UDP (Linux).

Ativar os usuários não raiz para adicionar nós

Se o servidor do SSH desativar o logon do usuário raiz, é possível ativar o logon do usuário não raiz para adicionar nós. Quando você ativa as credenciais de logon do usuário não raiz, a caixa de diálogo Adicionar o nó é alterada e exibe a opção Credencial raiz.

Observação: se você alterar as credenciais do nó cliente de um usuário raiz para um usuário não raiz, é recomendável que você limpe a pasta */tmp* no nó cliente antes de executar a tarefa de backup.



Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o arquivo server.cfg a partir do seguinte local:

   `/opt/Arcserve/d2dserver/configfiles/server.cfg`

   Observação: se o arquivo server.cfg não estiver presente, crie-o.

3. Adicione a seguinte linha ao arquivo server.cfg para ativar a função de usuário não raiz:

   `enable_non_root_user=true`

   A função de usuário não raiz é ativada.

4. (Opcional) Adicione a seguinte linha ao arquivo server.cfg para desativar a função de usuário não raiz:

   ```
   enable_non_root_user=false
   ```

   A função de usuário não raiz é desativada.

   Os usuários não raiz são ativados para adicionar nós.

   Observação: se você alterar a senha do usuário raiz ou do usuário não raiz e, em seguida, modificar o nó, você deve digitar novamente tanto a senha raiz, quanto a senha não raiz em seus respectivos campos na caixa de diálogo Modificar nó.

   Observação: os usuários não raiz não podem gerenciar nós usando o comando *d2d-node* a partir da linha de comando.

Como configurar a conta de usuário sudo para nós do Linux

É possível usar sudo para configurar contas de usuário comum para executar tarefas de backup e restauração. Para contas sudo, todas as configurações se relacionam a nós do Linux. Quando a conta sudo é configurada corretamente, é possível usá-la de modo semelhante a uma conta raiz normal em todas as interfaces de usuário. Usando a conta sudo, você pode executar tarefas como: adicionar nós, fazer backup de nós, restaurar arquivos. Configure o sudo de acordo com o documento específico de distribuição do Linux.

Execute essas tarefas para gerenciar os usuários sudo:

- Verificar os pré-requisitos
- Modificar as configurações Sudo padrão no SUSE
- Configurar o sudo no Debian
- Configurar o Sudo para conceder autorização sem senha ao usar a autenticação de chave pública SSH
- Configurar o Sudo para permitir somente processo do agente de backup

Verificar os pré-requisitos

Considere os pré-requisitos a seguir antes de gerenciar os usuários não raiz:

- Você possui credenciais de logon raiz para o nó Linux.
- Certifique-se de configurou corretamente a permissão do sudo para o usuário desejado.
  - Certifique-se de que o usuário sudo tem permissão para executar pelo menos estes programas: d2d_ea e ln. Por exemplo, se o nome de usuário for backupadmin, o exemplo de configuração do sudo será: *backupadmin ALL=(ALL) /usr/bin/d2d_ea,/usr/bin/ln*.
  - Verifique se o usuário sudo tem permissão para manter pelo menos as seguintes variáveis de ambiente:

NOMEDOHOST	USERNAME	LANG	LC_ADDRESS
LC_CTYPE	LC_COLLATE	LC_ IDENTIFICATION	LC_ MEASUREMENT
LC_MESSAGES	LC_MONETARY	LC_NAME	LC_NUMERIC
LC_TIME	LC_ALL LANGUAGE	SSH_ CONNECTION	CRE_ROOT_ PATH
CRE_LOG_BASE_ DIR	TARGET_BOOTSTRAP_ DIR	TARGET_WORK_ DIR	ID da tarefa

Por exemplo, se o nome de usuário for backupadmin, os exemplos de configuração do sudo serão:

Padrões: backupadmin env_keep += "HOSTNAME USERNAME LANG LC_ADDRESS LC_CTYPE"

Padrões: backupadmin env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT"

Padrões: backupadmin env_keep += "LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC LC_TIME LC_ALL LANGUAGE"

Padrões: backupadmin env_keep += "SSH_CONNECTION CRE_LOG_ BASE_DIR jobID TARGET_BOOTSTRAP_DIR CRE_ROOT_PATH TARGET_ WORK_DIR"

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Modificar as configurações Sudo padrão no SUSE

Por padrão, o SUSE exige uma senha raiz, em vez da senha do usuário, para conceder autorização. Uma autenticação Sudo não funciona no servidor de backup Linux, pois o servidor de backup usa as credenciais do usuário para conceder autorização. É possível modificar as configurações padrão do sudo para autorizar o uso de credenciais de usuário.

Siga estas etapas:

1. Efetue logon no nó Linux como um usuário raiz.
2. Abra o arquivo **/etc/sudoer** ou execute o comando *visudo*.
3. Digite um comentário sobre as configurações como mostrado no exemplo a seguir.

   Exemplo:

   ```
   #Defaults targetpw # solicitar a senha do usuário de destino, por exemplo, raiz

   #ALL ALL=(ALL) ALL # WARNING! Só use essa opção junto com "'Defaults targetpw".
   ```

4. Verifique se a linha de comando sudo agora requer uma senha de usuário, em vez da senha raiz para conceder autorização.

   Você modificou as configurações padrão do sudo com êxito.

Configurar o sudo no Debian

Por padrão, a conta raiz não está ativada para logon no Debian. Como resultado, é necessária uma autenticação sudo quando você adiciona o Debian Linux como um nó do Linux.

Siga estas etapas:

1. Efetue logon no nó do Linux e acesse a raiz usando o comando *su*.
2. Se o sudo não estiver instalado, instale o pacote sudo usando o seguinte comando:

   ```
   apt-get install sudo
   ```

3. Adicione um usuário existente com a ID “user” ao grupo “sudo”:

   Exemplo:

   ```
   adduser user sudo
   ```

   ou crie um usuário com o sudo:

   ```
   adduser user
   ```

   ```
   adduser user sudo
   ```

4. Faça logon no shell do usuário e digite o seguinte comando para verificar se o usuário tem autorização:

   ```
   sudo -v
   ```

   Você configurou o sudo com êxito no Debian.

Configurar o Sudo para conceder autorização sem senha ao usar a autenticação de chave pública SSH

Ao usar a autenticação de chave pública SSH, o servidor de backup Linux não armazena as credenciais do usuário. É possível configurar o Sudo para permitir a autorização sem senha.

Siga estas etapas:

1. Efetue logon no nó Linux como um usuário raiz.
2. Abra o arquivo **/etc/sudoer** ou execute *visudo* para editar o arquivo de configuração.
3. Vá para a linha de configuração do usuário especificado e adicione a opção "NOPASSWD".

   Por exemplo, se o nome de usuário for backupadmin, adicione a opção "NOPASSWD" conforme mostrado no exemplo a seguir:

   Exemplo: backupadmin ALL=(ALL) NOPASSWD: /usr/bin/d2d_ea,/user/bin/ln
4. Efetue logon no shell de usuário e digite o seguinte comando para verificar se a autorização não exige senha:

   ```
   sudo -v
   ```

   Você configurou sudo com êxito, para conceder autorização sem senha quando estiver usando a configuração da chave pública SSH.

Configurar o Sudo para permitir somente processo do agente de backup

Quando o usuário só tem permissão para usar comandos limitados em sudo, é necessário realizar a instalação manual do programa do agente de backup. Para que as tarefas de backup sejam executadas, é necessário ter a permissão do sudo para o processo *d2d_ea*.

Siga estas etapas:

1. Efetue logon no nó Linux como um usuário raiz.
2. Abra o arquivo **/etc/sudoer** ou execute *visudo* para editar o arquivo de configuração.
3. Navegue até a linha de configuração para o usuário especificado e adicione '/usr/-bin/d2d_ea' ao item de configuração dos comandos permitidos.

   Por exemplo, se o nome de usuário for backupadmin, adicione a opção '/usr/-bin/d2d_ea' conforme mostrado no exemplo a seguir:

   Exemplo: backupadmin ALL=(ALL) /usr/bin/d2d_ea
4. Determine se o nó da origem do backup é de 32 ou 64 bits e localize o binário correto no servidor do agente de backup:
5. Copie o binário determinado na etapa 4 no nó da origem do backup como d2d_ea e, em seguida, coloque em '/usr/bin/d2d_ea'.

   ```
   Para 32 bits: /opt/Arcserve/d2dserver/sbin/ea.32
   ```

   ```
   Para 64 bits: /opt/Arcserve/d2dserver/sbin/ea.64
   ```
6. Execute o seguinte comando para verificar a permissão de execução:

   ```
   chmod +x /usr/bin/d2d_ea
   ```

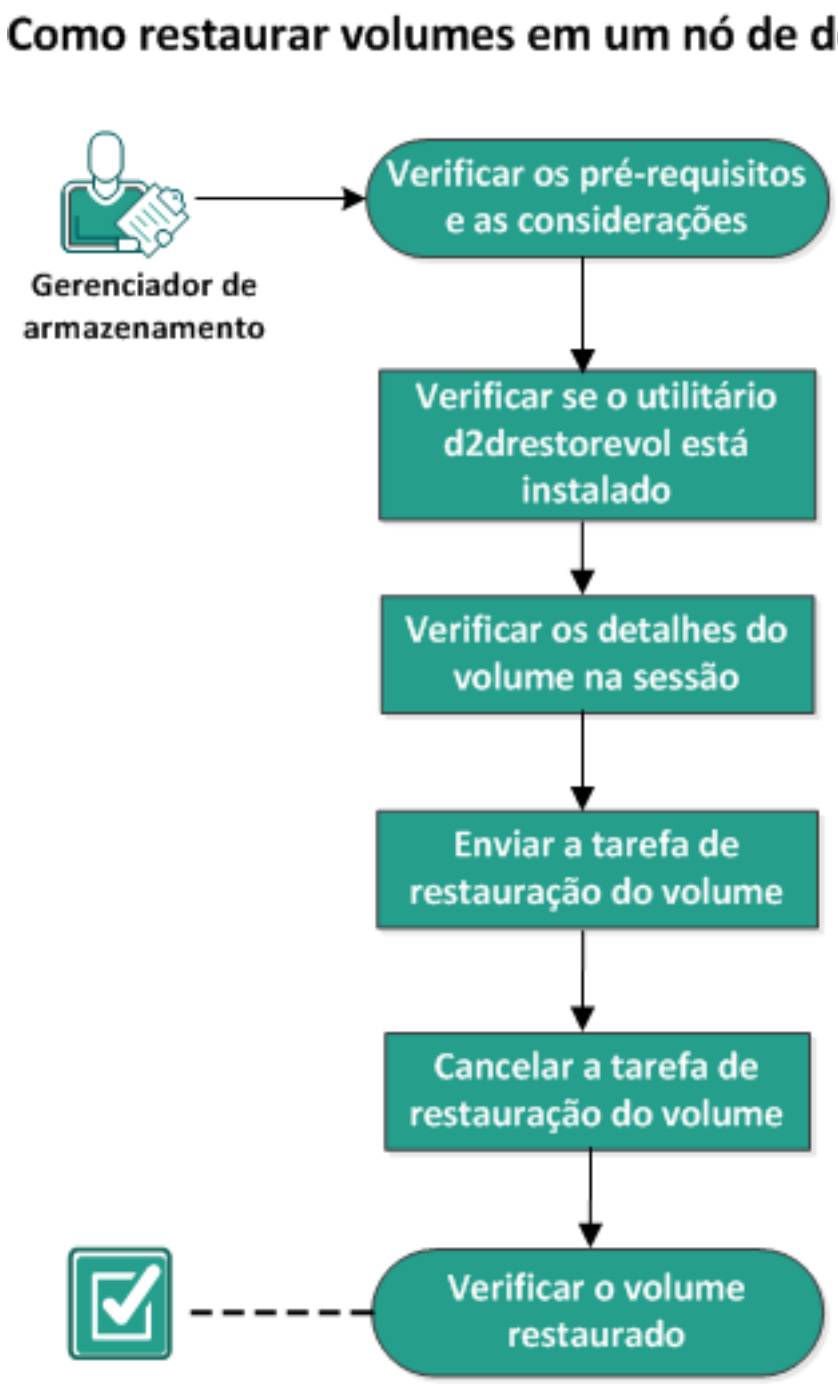
   Você conseguiu configurar o Sudo para permitir somente o processo do agente de backup.

Como restaurar volumes em um nó de destino

É possível restaurar os volumes individuais no nó de destino sem executar uma BMR completa. O nó de destino pode ser um servidor de backup ou um nó protegido.

A restauração de volumes individuais utiliza menos recursos e oferece melhor desempenho.

O diagrama a seguir exibe o processo para restaurar volumes:



Execute as tarefas a seguir para restaurar volumes:

- Verificar os pré-requisitos e as considerações
- Verificar se o utilitário d2drestorevol está instalado
- Verificar os detalhes do volume na sessão
- Enviar a tarefa de restauração do volume
- Cancelar a tarefa de restauração do volume
- Verificar o volume restaurado

Verificar os pré-requisitos e as considerações

Verifique os seguintes pré-requisitos antes de restaurar volumes:

- Você tem uma sessão de backup válida para executar uma restauração.
- A restauração de volume oferece suporte a sessão gerada pelos planos ou tarefas com base em agente Linux.
- As sessões de backup devem ser acessadas localmente no nó de destino. Se o local da sessão estiver no volume local do nó de destino, use o mesmo caminho de diretório que o local da sessão. Se o local da sessão estiver em um compartilhamento de rede, primeiro monte o compartilhamento de rede em um ponto de montagem local e, em seguida, use o caminho do ponto de montagem como o local da sessão. Se a sessão é obtida em backup para um repositório de dados do RPS, primeiro encontre o caminho compartilhado em detalhes do repositório de dados. Em seguida, monte o caminho compartilhado de um ponto de montagem local e use o caminho do ponto de montagem como o local da sessão.
- Os volumes de destino que deseja restaurar devem ser desmontados, usando o comando umount:

  ```
  Exemplo: umount /dev/sda2
  ```

- O volume de destino deve ser igual ou maior que o volume de origem.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Verifique as considerações a seguir antes de restaurar volumes:

- Durante a restauração, os dados existentes no volume de destino serão apagados. Execute um backup de seus dados existentes no volume de destino antes da restauração.

Verificar se o utilitário d2drestorevol está instalado

O utilitário d2drestorevol restaura o volume no nó de destino. O nó de destino pode ser um servidor de backup ou qualquer outro nó do Linux (cliente). Se o utilitário restorevol não estiver instalado no nó de destino, você deverá instalá-lo manualmente.

Restaurar em um servidor de backup

Se o nó de destino for um servidor de backup, significa que o utilitário já foi instalado com o pacote de instalação. Verifique se o utilitário está presente na pasta *bin*.

Siga estas etapas:

1. Efetue logon no servidor de backup.
2. Verifique se o utilitário está localizado no seguinte local:

   ```
   /opt/Arcserve/d2dserver/bin/d2drestorevol
   ```

   O utilitário é instalado e verificado.

Restaurar em um cliente

Um nó cliente não terá o utilitário instalado nele. Você precisa instalar manualmente o utilitário no cliente.

Importante: O download do utilitário deve ser feito a partir do servidor de backup, conforme descrito nas etapas a seguir. Se copiar manualmente o utilitário para um cliente de um servidor de backup, ele poderá não funcionar corretamente.

Siga estas etapas:

1. Efetue logon no cliente.
2. Localize o caminho de download do utilitário d2drestorevol na linha de comando.

   ```
   http[s]://[Backup-Server-address]:[port]/d2drestorevol
   ```

3. Faça download do script usando uma ferramenta de linha de comando, como wget.

   ```
   wget http://192.168.1.1:8014/d2drestorevol –O d2drestorevol
   ```

   Observação: se o arquivo server.cfg não estiver presente, crie-o.

   ```
   wget https://192.168.1.1:8014/d2drestorevol -O d2drestorevol
   --no-check-certificate
   ```

4. Forneça a autorização de execução para o utilitário usando o seguinte comando:

   ```
   chmod +x d2drestorevol
   ```

A permissão é fornecida.

O d2drestorevol é instalado e verificado.

Verificar os detalhes do volume na sessão

Verifique os detalhes do volume na sessão que deseja restaurar. É possível ver o volume de origem, o sistema de arquivos, o tamanho de arquivo, além de informações de montagem na saída.

Siga estas etapas:

1. Efetue logon no nó de destino.
2. Se os pontos de recuperação estiverem em uma pasta local ou compartilhada, use o seguinte comando para verificar as informações de volume:

   ```
   d2drestorevol --command=info --storage-path=<local_path> --
   node=<node_name> --rp=<recovery_point>
   ```

   --command=info

   Especifica se os detalhes da sessão de volume serão exibidos.

   --storage-path

   Especifica o caminho determinado no tópico Pré-requisitos. Para obter mais informações, consulte Verificar os pré-requisitos e considerações.

   --node

   Especifica o nó de origem do qual foi feito o backup.

   --rp

   Especifica o ponto de recuperação ou sessão de recuperação que deseja restaurar. Em geral, o ponto de recuperação está no seguinte formato: S00000000X, em que X é um valor numérico.

   A saída é exibida.

3. Se os pontos de recuperação estiverem em um repositório de dados de RPS, use o seguinte comando para verificar as informações de volume:

   ```
   d2drestorevol --command=info --storage-path=<rps_path> --
   node="<node_name>[UUID_number]" --rp=<recovery_point> --rps-
   host=<host_name> --rps-user=<user_name> --rps-pw=<rps_
   password> --rps-protocal=<internet_secutity_protocol> --rps-
   port=<port_number> --rps-dedup
   ```

   O comando a seguir é um exemplo de um repositório de dados ativado para a redução de redundância:

   ```
   d2drestorevol --command=info --storage-path=/root/rpsshare -
   -node="xx.xx.xx.xx[11111aa-22bb-33cc-yyyy-4c4c4c4c]" --
   ```

```
rp=VStore/S0000000001 --rps-host=machine_name --rps-user-
r=administrator --rps-pw=******** --rps-protocol=https --
rps-port=8014 --rps-dedup
```

--command=info

Especifica se os detalhes da sessão de volume serão exibidos.

--storage-path

Especifica o caminho determinado no tópico Pré-requisitos. Para obter mais informações, consulte Verificar os pré-requisitos e considerações.

--node

Especifica o nó de origem do qual foi feito o backup no seguinte formato:

<nome do nó>[<uuid>]

--rp

Especifica o ponto de recuperação ou a sessão de recuperação que você deseja restaurar a partir de um repositório de dados de RPS. Em geral, uma sessão de ponto de recuperação de um repositório de dados do RPS deve ser especificada no seguinte formato:

VStore/S00000000X, onde X é um valor numérico.

-- rps-host

Especifica o nome do host do RPS em que a sessão de recuperação está armazenada.

-- rps-user

Especifica o nome do usuário para acessar o host do RPS.

-- rps-pw

Especifica a senha para acessar o host do RPS.

-- rps-protocol

Especifica o protocolo para o host do RPS. O protocolo é http ou https.

-- rps-port

Especifica o número da porta do host do RPS.

-- rps-dedup

Especifica que o repositório de dados está com a redução de redundância ativada. Esse parâmetro é necessário apenas quando o repositório de dados tiver ativado a redução de redundância.

-- ds-share-folder

Especifica o caminho compartilhado do repositório de dados. Esse parâmetro é necessário apenas quando o repositório de dados tiver desativado a redução de redundância.

-- ds-user

Especifica o nome do usuário para acessar o caminho compartilhado do repositório de dados.

-- ds-user-pw

Especifica o nome do usuário para acessar o caminho compartilhado do repositório de dados.

-- ds-pw

Especifica a senha de criptografia de dados se o repositório de dados também tiver ativado a criptografia.

A saída é exibida.

Os detalhes do volume são verificados.

Enviar a tarefa de restauração do volume

Envie o a tarefa de restauração de volume para iniciar a restauração do volume no nó de destino.

Siga estas etapas:

1. Efetue logon no nó de destino.
2. Se os pontos de recuperação estiverem em uma pasta local ou em uma rede compartilhada, envie a tarefa de restauração usando o seguinte comando:

```
d2drestorevol --command=restore  --storage-path=<local_
path> --node=<node_name> --rp=<recovery_point> --source-
volume=<source_volume> --target-volume=<target_volume>
[--encryption-password=<encryption_password>] [--mount-
target=<mount_point> [--quick-recovery]]
```

-command=restore

Especifica que a tarefa de restauração do volume foi enviada.

--storage-path

Especifica o caminho determinado no tópico Pré-requisitos. Para obter mais informações, consulte Verificar os pré-requisitos e considerações.

--node

Especifica o nó de origem do qual foi feito o backup.

--rp

Especifica o ponto de recuperação ou sessão de recuperação que deseja restaurar. Em geral, o ponto de recuperação está no seguinte formato: S00000000X, em que X é um valor numérico.

--encryption-password

Especifica a senha da sessão. Esta opção é obrigatória se a sessão for criptografada. Se a sessão for criptografada, mas essa opção não estiver presente, você será solicitado a digitar a senha a partir de um terminal.

--source-volume

Especifica o volume de origem. É possível obter o volume de origem usando o parâmetro *comando=info*, conforme descrito em Verificar os detalhes do volume no tópico Sessão ou o volume de origem poderá ser o ponto de montagem do sistema de origem.

--target-volume

Especifica o caminho do arquivo do dispositivo do nó de destino.

Exemplo: /dev /sda2

--mount-target

Especifica o ponto de montagem onde o volume restaurado deve ser montado.

Exemplo: /mnt/volrestore

--quick-recovery

Quando usado junto com "--mount-target" , o volume de destino será montado assim que possível. É possível usar os dados no volume de destino enquanto os dados estão sendo restaurados.

Depois que a tarefa de restauração for concluída, o processo de restauração encerra automaticamente e você pode continuar usando os dados sem qualquer interrupção.

Observação: quando uma tarefa de restauração de volume, e a tarefa de backup são executadas ao mesmo tempo, então:

- Se --quick-recovery for usado, a tarefa (de restauração de volume ou de backup) que inicia mais tarde não será executada.
- Se --quick-recovery não for usado, a tarefa de backup fará o backup apenas dos volumes que não estão sendo restaurados.

A tarefa de restauração é enviada e uma tela é aberta exibindo o andamento da operação. Se desejar enviar outras tarefas, você pode aguardar até que a tarefa atual seja concluída ou pressionar Q para sair da tela e, em seguida, enviar uma nova tarefa.

3. Se os pontos de recuperação estiverem em um repositório de dados do RPS, envie a tarefa de restauração usando o seguinte comando:

```
d2drestorevol --command=restore --storage-path=<local_path>
--node=<node_name> --rp=<recovery_point> --source-volu-
me=<source_volume> --target-volume=<target_volume> [--encryp-
tion-password=<encryption_password>] [--mount-target=<mount_
point> [--quick-recovery]]
```

--command=restore

Especifica que a tarefa de restauração do volume foi enviada.

--storage-path

Especifica o caminho determinado no tópico Pré-requisitos. Para obter mais informações, consulte Verificar os pré-requisitos e considerações.

--node

Especifica o nó de origem do qual foi feito o backup no seguinte formato:

<nome do nó>[<uuid>]

--rp

Especifica o ponto de recuperação ou a sessão de recuperação que você deseja restaurar de um repositório de dados no RPS. Em geral, uma sessão de ponto de recuperação de um repositório de dados do RPS deve ser especificada no seguinte formato:

VStore/S00000000X, onde X é um valor numérico.

--source-volume

Especifica o volume de origem. É possível obter o volume de origem usando o parâmetro *comando=info*, conforme descrito em Verificar os detalhes do volume no tópico Sessão ou o volume de origem poderá ser o ponto de montagem do sistema de origem.

--target-volume

Especifica o caminho do arquivo do dispositivo do nó de destino.

Exemplo: /dev /sda2

-- rps-host

Especifica o nome do host do RPS em que as sessões de recuperação estão armazenadas.

-- rps-user

Especifica o nome do usuário para acessar o host do RPS.

-- rps-pw

Especifica a senha para acessar o host do RPS.

-- rps-protocol

Especifica o protocolo para o host do RPS. O protocolo é http ou https.

-- rps-port

Especifica o número da porta do host do RPS.

-- rps-dedup

Especifica que o repositório de dados ativou a redução de redundância. Esse parâmetro é necessário apenas quando o repositório de dados tiver ativado a redução de redundância.

-- ds-share-folder

Especifica o caminho compartilhado do repositório de dados. Esse parâmetro é necessário apenas quando o repositório de dados tiver desativado a redução de redundância.

-- ds-user

Especifica o nome do usuário para acessar o caminho compartilhado do repositório de dados.

-- ds-user-pw

Especifica a senha para acessar o caminho compartilhado do repositório de dados.

-- ds-pw

Especifica a senha de criptografia de dados se o repositório de dados também tiver ativado a criptografia.

A tarefa de restauração é enviada e uma tela é aberta exibindo o andamento da operação. Se desejar enviar outras tarefas, você pode aguardar até que a tarefa atual seja concluída ou pressionar Q para sair da tela e, em seguida, enviar uma nova tarefa.

4. (Opcional) Use o comando a seguir para ver o andamento da tarefa de restauração do volume:

```
d2drestorevol --command=monitor
```

Os detalhes do progresso, como o nome do volume, o tempo decorrido, o andamento, a velocidade, o status e o tempo restante, são exibidos em uma tela.

A tela é fechada quando a tarefa é concluída. Também é possível pressionar Q para sair manualmente da tela. Sair manualmente da tela não interrompe a tarefa de restauração em andamento.

A tarefa de restauração de volume será enviada.

Cancelar a tarefa de restauração do volume

É possível cancelar a tarefa de restauração de volume a partir da linha de comando do nó de destino. Use o seguinte comando para cancelar a tarefa de restauração de volume.

```
d2drestorevol --command=cancel --target-volume=<target_
volume>
```

--command=cancel

Especifica se a tarefa de restauração do volume foi cancelada.

--target-volume

Especifica o caminho do arquivo do dispositivo do nó de destino. O valor deve ser idêntico ao valor usado para enviar a tarefa de restauração.

Importante: o cancelamento de uma tarefa de restauração do volume fará com que o volume de destino não possa mais ser usado. Nesses casos, você pode tentar novamente executar a tarefa de restauração do volume ou restaurar os dados perdidos, se você possuir um backup.

Verificar o volume restaurado

Verifica os dados quando o volume é restaurado.

Siga estas etapas:

1. Efetue logon no nó de destino.
2. Revise a tela de andamento para verificar o status de conclusão.
3. (Opcional) Analise o arquivo *2drestvol_activity_[target volume].log* para ver todos os logs da tarefa de restauração.
4. Monte o volume restaurado e verifique se os dados foram restaurados.

A tarefa de restauração do volume é verificada.

O volume é restaurado com êxito.

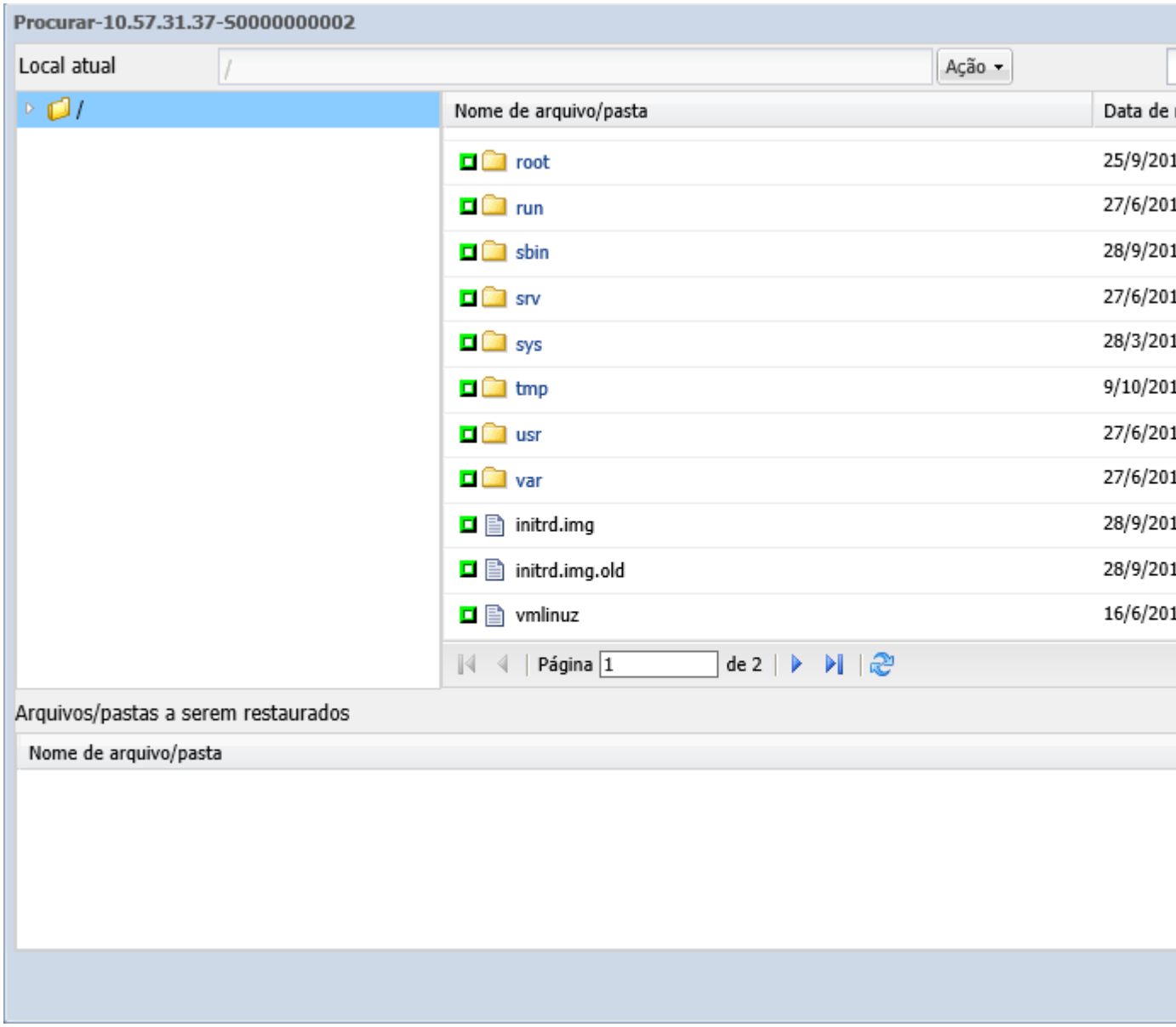
Como fazer download de arquivos/pastas sem restaurar para nós do Linux

[[[Undefined variable Variables.AUDP]]] permite que você faça download de um arquivo ou uma pasta completa sem enviar para restauração. No Assistente de restauração, a tela Procurar pontos de recuperação permite fazer download diretamente de qualquer arquivo ou pasta completa com todos os arquivos. Fazer download antes da restauração pode ajudar a executar uma verificação rápida de arquivos para evitar que arquivos indesejados sejam restaurados.

Um único arquivo é transferido por download diretamente no mesmo formato, enquanto uma pasta é transferida por download como um arquivo zip. O arquivo zip tem o seguinte formato de nome:

[nodename]_[sessionid]_[timestamp].zip

Para fazer download, basta acessar a tela Procurar pontos de recuperação no Assistente de restauração. A captura de tela a seguir mostra como fazer download de um arquivo ou pasta para nós do Linux:



Para abrir os arquivos baixados, use ferramentas de compactação como WinZip, WinRAR, 7-Zip, etc.

Como restaurar um banco de dados Oracle usando o Agente do Arcserve UDP (Linux)

É possível restaurar todo o banco de dados Oracle ou restaurar arquivos específicos do banco de dados. Também é possível executar uma BMR (Bare Metal Recovery – Recuperação Bare Metal) de um Oracle Server quando o servidor de origem não estiver funcionando corretamente. Caso tenha perdido o banco de dados e deseja tê-lo disponível de imediato, é possível executar uma recuperação instantânea. Leia os pré-requisitos para cada tipo de restauração, antes de iniciar o processo de restauração.

O diagrama a seguir ilustra o processo de restauração de um banco de dados Oracle usando o Agente do Arcserve UDP (Linux):

Siga estas etapas para restaurar um banco de dados Oracle usando o Agente do Arcserve UDP (Linux):

- Executar uma recuperação bare metal de um Oracle Server
- Execute uma recuperação instantânea de um banco de dados Oracle
- Execute Recuperação granular de um banco de dados Oracle

Execute uma recuperação bare metal (BMR) de um Oracle Server

Uma BMR restaura o sistema operacional e os aplicativos de software e recupera todos os dados incluídos no backup. A BMR é o processo de restauração de um sistema de computador do estado bare metal. Bare metal é um computador sem sistema operacional, drivers e aplicativos de software. Depois que a restauração for concluída, o computador de destino será reinicializado automaticamente no mesmo ambiente operacional que o nó de origem do backup e todos os dados serão restaurados.

É possível executar uma BMR usando o endereço IP ou o endereço MAC (Media Access Control – Controle de Acesso à Mídia) do computador de destino. Se você inicializar o computador de destino usando o Live CD do Agente do Arcserve UDP (Linux), será possível obter o endereço IP do computador de destino.

Verificar os pré-requisitos

Verifique os seguintes pré-requisitos antes de restaurar o banco de dados Oracle:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Você tem um computador de destino válido para a BMR.
- Certifique-se de que criou o Live CD do Agente do Arcserve UDP (Linux) (Linux).
- Se você deseja executar uma BMR usando o endereço IP, deve obter o endereço IP do computador de destino usando o Live CD.
- Se você deseja executar uma BMR com base em PXE usando o endereço MAC, deve ter o endereço MAC do computador de destino.
- O banco de dados Oracle armazena todos os arquivos relacionados ao banco de dados (arquivos de dados, logs de repetição, logs arquivados, pfile, spfile, backups) em ext2, ext3, ext4 e ReiserFS. O banco de dados não reconhece o OCFS /OCFS2 (Oracle Cluster File System), discos não processados ou sistemas de arquivos ASM (Automatic Storage Management).
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Restaurar um Oracle Server

Se o Oracle Server estiver danificado, é possível restaurar todo o servidor executando uma BMR.

Siga estas etapas:

1. Efetue logon no console do servidor de backup Linux como usuário raiz.
2. Execute uma recuperação bare metal usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte o Como executar uma recuperação bare metal (BMR) para máquinas Linux.
3. Após a conclusão da tarefa de BMR, efetue logon no computador de destino e certifique-se de que o banco de dados esteja restaurado.

   O Oracle Server é recuperado com êxito.

Não há suporte do destino da memória no Oracle Server restaurado

Sintoma

Eu executei uma recuperação bare metal de um Oracle Server. O tamanho da memória do computador de destino é menor do que o Oracle Server de origem e o banco de dados do Oracle utiliza AMM (Automatic Memory Management). Após a BMR, quando eu inicio a instância do banco de dados Oracle, recebo o seguinte erro:

SQL> startup

ORA-00845: MEMORY_TARGET não suportado nesse sistema

Solução

Para resolver esse erro, aumente o tamanho do sistema de arquivos virtual de memória compartilhada.

Siga estas etapas:

1. Efetue logon no computador de destino como um usuário raiz.
2. Abra o prompt de comando e verifique o tamanho do sistema de arquivos virtual de memória compartilhada.

   ```
   # df -k /dev/shm

   Filesystem 1K-blocks Used Available Use% Mounted on tmpfs
   510324 88 510236 1% /dev/shm
   ```

3. Digite o seguinte comando e especifique o tamanho necessário da memória compartilhada:

   ```
   # mount -o remount,size=1200m /dev/shm
   ```

4. Navegue para a pasta "/etc/fstab" e atualize a configuração tmpfs:

   ```
   tmpfs /dev/shm tmpfs size=1200m 0 0
   ```

   Observação: o tamanho do sistema de arquivos virtual de memória compartilhada deve ser grande o suficiente para acomodar os valores MEMORY_TARGET e MEMORY_MAX_TARGET. Para obter mais informações sobre as variáveis, consulte a documentação do Oracle.

Execute uma recuperação instantânea de um banco de dados Oracle

É possível recuperar instantaneamente um banco de dados Oracle sem executar uma BMR completa. É possível recuperar o banco de dados com comandos específicos da linha de comando.

Verificar os pré-requisitos

Verifique os seguintes pré-requisitos antes de restaurar o banco de dados Oracle:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- As sessões de backup devem ser acessadas localmente no nó de destino. Se o local da sessão estiver no volume local do nó de destino, use o mesmo caminho de diretório que o local da sessão. Se o local da sessão estiver em um compartilhamento de rede, primeiro monte o compartilhamento de rede em um ponto de montagem local e, em seguida, use o caminho do ponto de montagem como o local da sessão.
- Os volumes de destino que deseja restaurar não podem ser um volume raiz e devem ser desmontados usando o comando unmount.

  Exemple: umount /dev/sda1
- O volume de destino deve ser igual ou maior que o volume de origem.
- O banco de dados Oracle armazena todos os arquivos relacionados ao banco de dados (arquivos de dados, logs de repetição, logs arquivados, pfile, spfile, backups) em ext2, ext3, ext4 e ReiserFS. O banco de dados não reconhece o OCFS /OCFS2 (Oracle Cluster File System), discos não processados ou sistemas de arquivos ASM (Automatic Storage Management).
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Restaurar o banco de dados instantaneamente

Ao recuperar o banco de dados instantaneamente, o banco de dados está disponível para uso imediato. Entretanto, o processo de recuperação é executado em back-end e todos os arquivos ficam disponíveis somente depois que o banco de dados é recuperado completamente.

Observação: para obter mais informações sobre restauração de volume, consulte o tópico Como restaurar volumes em um nó de destino.

Siga estas etapas:

1. Efetue logon no computador de destino como um usuário raiz.
2. Abra um prompt de comando como um usuário raiz.
3. Verifique se o volume de destino /dev/sdb1 não está montado.

   ```
   # df | grep 'target_volume'
   ```

   Exemplo: # df | grep '/dev/sdb1'

4. Monte o compartilhamento de NFS remoto para o caminho local.

   ```
   #mount <nfs_session_path>:/nfs <session_location_on_local>
   ```

   Exemplo: #mount xxx.xxx.xxx.xxx:/nfs /CRE_ROOT

5. Insira o seguinte comando para iniciar a tarefa de restauração:

   ```
   #. /d2drestorevol --command=restore --storage-path=<session_
   location_on_local> --node=<oracle_server> --rp=last --
   source-volume=<mount_point_for_oracle_data_volume> --target-
   volume=<restore_target_volume_name> --mount-target=<mount_
   point_for_oracle_data_volume> --quick-recovery
   ```

   Exemplo: #. /d2drestorevol --command=restore --storage-path=/CRE_ROOT --node-e=rh63-v2 --rp=last --source-volume=/opt/oracle --target-volume=/dev/sdb1 --mount-target=/opt/oracle --quick-recovery

   É possível iniciar o banco de dados Oracle imediatamente após o início da tarefa de restauração. Você não precisa aguardar a conclusão da recuperação do banco de dados.

6. Abra outro prompt de comando e efetue logon com o nome de usuário e a senha do Oracle.

   ```
   $sqlplus / as sysdba

   SQL>startup;
   ```

Exemplo: #. /d2drestorevol --command=restore --storage-path=/CRE_ROOT --node-e=rh63-v2 --rp=last --source-volume=/opt/oracle --target-volume=/dev/sdb1 --mount-target=/opt/oracle --quick-recovery

O banco de dados Oracle é aberto e você pode realizar as operações de banco de dados normais, como consultar, inserir, excluir, atualizar dados, e assim por diante.

O banco de dados Oracle foi instantaneamente recuperado.

Execute Recuperação granular de um banco de dados Oracle

É possível restaurar arquivos específicos relacionados ao banco de dados Oracle. Esses arquivos podem ser arquivos de controle, arquivos de dados de espaços para tabelas.

Verificar os pré-requisitos

Verifique os seguintes pré-requisitos antes de restaurar o banco de dados Oracle:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver.
- Você tem um nó de destino válido para recuperar os dados.
- Você verificou se o servidor de backup do Linux oferece suporte ao sistema de arquivos que deseja restaurar.
- O banco de dados Oracle armazena todos os arquivos relacionados ao banco de dados (arquivos de dados, logs de repetição, logs arquivados, pfile, spfile, backups) em ext2, ext3, ext4 e ReiserFS. O banco de dados não reconhece o OCFS /OCFS2 (Oracle Cluster File System), discos não processados ou sistemas de arquivos ASM (Automatic Storage Management).
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Restaurar espaços para tabelas

Se um espaço para tabelas do banco de dados for perdido ou danificado, é possível restaurá-lo executando uma recuperação em nível de arquivo. Após a recuperação em nível de arquivo ser bem-sucedida, você precisa recuperar manualmente o espaço para tabelas.

Siga estas etapas:

1. Efetue logon no computador de destino como um usuário raiz.
2. Certifique-se de que o banco de dados esteja disponível.
3. Deixe offline o espaço para tabelas necessário.

   Exemplo: considere que o nome do espaço para tabelas seja MYTEST_DB. Digite o comando a seguir para deixar offline o espaço para tabelas:

   ```
   $ sqlplus "/ as sysdba"

   SQL> alter tablespace MYTEST_DB offline;
   ```

4. Liste todos os arquivos de dados do espaço para tabelas especificado MYTEST_DB.

   ```
   SQL> select file_name, tablespace_name from dba_data_files
   where tablespace_name='MYTEST_DB';

   FILE_NAME

   ----------------------------------------------------------------
   --------------------

   TABLESPACE_NAME

   ------------------------------

   /opt/oracle/oradata/lynx/MYTEST_DATA01.dbf

   MYTEST_DB
   ```

5. Restaure os arquivos de dados dos espaços para tabelas usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como executar uma recuperação em nível de arquivo em nós Linux.
6. Especifique as seguintes informações sobre o Assistente de restauração e envie a tarefa:

a. Ao selecionar os arquivos e as pastas, insira o nome do arquivo de dados necessário do espaço para tabelas e pesquisa.

Exemplo: insira "MYTEST_DATA01.dbf" do espaço para tabelas "MYTEST_DB" e pesquise.

b. Na página Computador de destino, especifique as seguintes informações:
   - Selecione Restaurar no local original.
   - Digite o nome do host ou o endereço IP do Oracle Server de destino.
   - Digite o nome de usuário raiz e a senha do Oracle Server de destino.
   - Selecione Substituir os arquivos existentes para a opção Resolvendo conflitos.

7. Após a restauração do arquivo de dados, recupere o espaço para tabelas do banco de dados Oracle.

   ```
   SQL>recover tablespace MYTEST_DB;

   Especificar log: {<RET>=suggested | filename | AUTO |
   CANCEL}

   Automático
   ```

8. Deixe online o espaço para tabela especificado.

   ```
   SQL>alter tablespace MYTEST_DB online;
   ```

   Agora, o espaço para tabelas está recuperado com êxito.

Restaurar arquivos de controle

Se os arquivos de controle do banco de dados forem perdidos ou danificados, é possível restaurá-los executando uma recuperação em nível de arquivo. Após a recuperação em nível de arquivo ser bem-sucedida, você precisa recuperar manualmente os arquivos de controle.

Siga estas etapas:

1. Efetue logon no computador de destino como um usuário raiz.
2. Encerre a instância do Oracle.

   ```
   SQL>shutdown abort
   ```

3. Inicie o banco de dados no estado nomount.

   ```
   SQL>startup nomount
   ```

4. Liste o caminho para todos os arquivos de controle.

   ```
   SQL> show parameter control_files;

   NAME            TYPE             VALUE

   -------------- -------- -------------

   control_files string /opt/oracle/oradata/lynx/control01.ctl,
   /opt/oracle/flash_recovery_area/lynx/control02.ctl
   ```

5. Restaure os arquivos de controle, usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como executar uma recuperação em nível de arquivo em nós Linux.
6. Especifique as seguintes informações sobre o Assistente de restauração e envie a tarefa:
   a. Ao selecionar os arquivos e as pastas, insira o nome do arquivo de controle necessário e pesquise. Repita esta etapa até que todos os arquivos de controle sejam selecionados.

      Exemplo: insira "control01.ctl" e pesquise.

   b. Na página Computador de destino, especifique as seguintes informações:
      - Selecione Restaurar no local original.
      - Digite o nome do host ou o endereço IP do Oracle Server de destino.
      - Digite o nome de usuário raiz e a senha do Oracle Server de destino.
      - Selecione Substituir os arquivos existentes para a opção Resolvendo conflitos.

7. Depois que todos os arquivos de controle forem restaurados, monte o banco de dados e abra-o.

   ```
   $sqlplus / as sysdba

   SQL>alter database mount;
   ```

8. Recupere o banco de dados com o comando RECOVER e adicione a cláusula USING BACKUP CONTROLFILE.

   ```
   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE
   ```

9. Aplique os logs arquivados solicitados.

   Observação: se o log arquivado necessário estiver ausente, isso indica que um registro de repetição necessário está localizado nos logs de repetição online. Isso ocorre porque as alterações não arquivadas estão localizadas nos logs online quando a instância falha. É possível especificar o caminho completo de um arquivo de log de repetição online e pressionar Enter (pode ser necessário executar isso algumas vezes até localizar o log correto).

   Exemplo:

   ```
   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE

   ORA-00279: alterar 1035184 gerado em 05/27/2014 18:12:49
   necessário para o segmento 1

   ORA-00289: suggestion :

   /opt/oracle/flash_recovery_area/LYNX/archivelog/2014_05_
   27/o1_mf_1_6_%u_.arc

   ORA-00280: change 1035184 for thread 1 is in sequence #6

   Especificar log: {<RET>=suggested | filename | AUTO |
   CANCEL}

   /opt/oracle/oradata/lynx/redo03,log

   Log aplicado.
   ```

10. Completa recuperação de mídia.
11. Abra o banco de dados com a cláusula RESETLOGS após concluir o processo de recuperação.

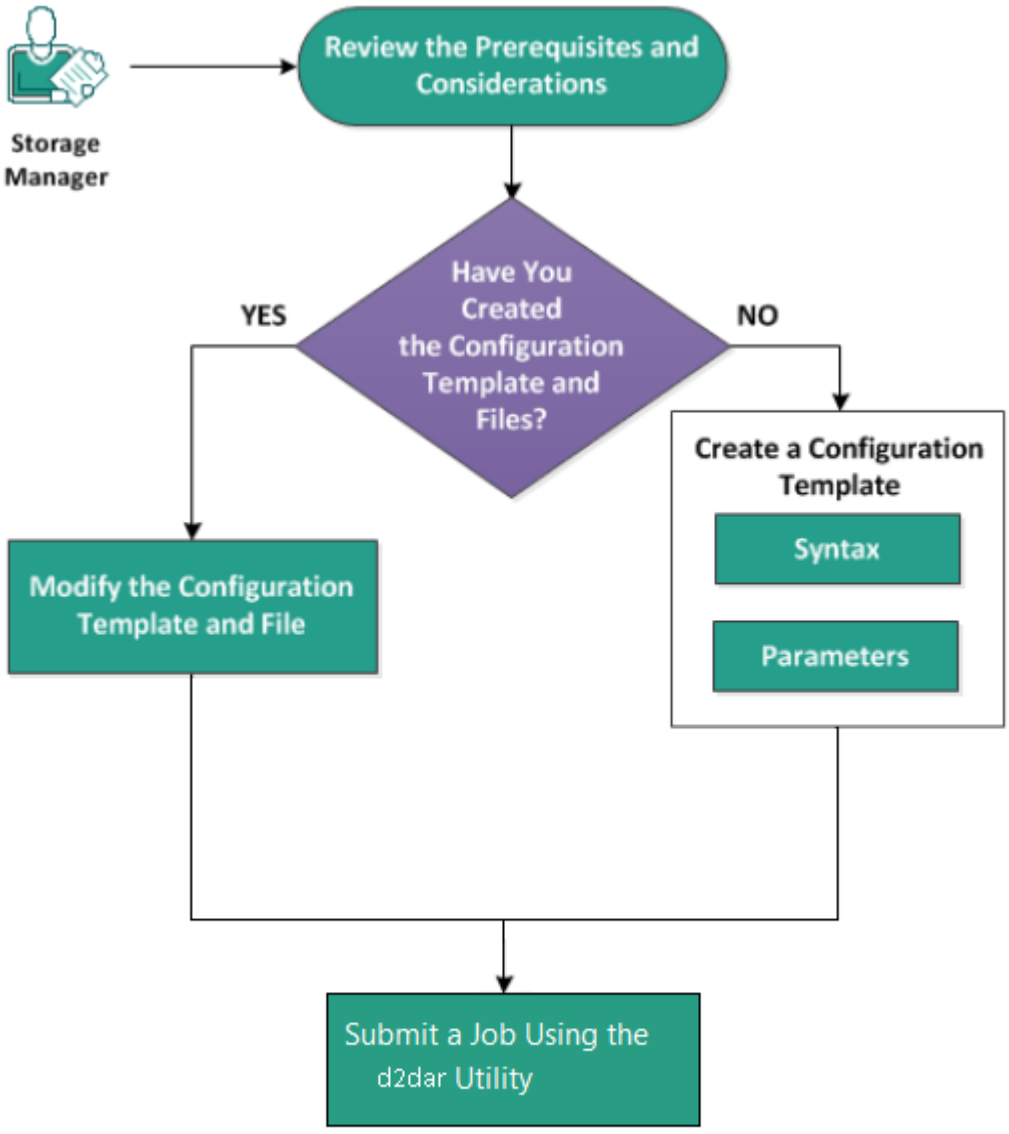
    ```
    SQL> alter database open resetlogs;
    ```

Os arquivos de controle são recuperados com êxito.

Como executar o teste de Recuperação garantida a partir da linha de comando

É possível executar o teste de Recuperação garantida a partir da linha de comando do servidor de backup usando o utilitário d2dar. O utilitário d2dar automatiza o processo de executar um Teste de recuperação garantida para sessões de backup especificadas.

O diagrama a seguir mostra o processo para executar o teste de Recuperação garantida a partir da linha de comando usando o utilitário d2dar:



Execute estas tarefas para executar o teste de Recuperação garantida:

- Verificar os pré-requisitos e as considerações
- Criar um modelo de configuração
- Modificar o arquivo e o modelo de configuração
- Enviar uma tarefa usando o utilitário d2dar

Verificar os pré-requisitos e as considerações

Revise as considerações a seguir antes de executar o teste de Recuperação garantida:

- As seguintes versões de hipervisores são suportadas para o teste de Recuperação garantida usando o utilitário d2dar:
  - VMware vCenter/ESX(i) 5.0 ou posterior
  - Windows Hyper-V Server 2012 ou posterior

    Observação: para saber mais sobre as máquinas virtuais Linux suportadas no Hyper-V, clique no link.
- O teste de Recuperação garantida só é executado a partir da linha de comando. A opção não está disponível na interface do usuário.

Criar um modelo de configuração

É possível criar um arquivo de configuração para permitir que o comando d2dar execute o teste de Recuperação garantida de acordo com os parâmetros especificados no arquivo.

Sintaxe

d2dar –createtemplate=<cfg_file_path>

O utilitário *d2dutil --encrypt* criptografa a senha e fornece uma senha criptografada. Você deve usar esse utilitário para criptografar todas as suas senhas.

Método 1

echo 'string' | ./d2dutil --encrypt

string é a senha que você especificar.

Método 2

Digite o comando *d2dutil –encrypt* e especifique sua senha. Pressione **Enter** e você poderá exibir o resultado na tela. Nesse método, a senha que digitar não será reproduzida na tela.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá para a pasta bin onde o Agente do Arcserve UDP para Linux está instalado, usando o seguinte comando:

   #cd /opt/Arcserve/d2dserver/bin
3. Crie o modelo de configuração usando o seguinte comando:

   #./d2dar --createtemplate=<cfg_file_path>

   <cfg_file_path> indica o local em que o modelo de configuração é criado.
4. Abra o modelo de configuração e atualize os seguintes parâmetros:

   job_name

   Especifica o nome da tarefa de Recuperação garantida.

   vm_name_prefix

   Especifica o prefixo da VM criado para a tarefa de Recuperação garantida. O nome da VM de Recuperação garantida é vm_name_prefix + nome do nó + carimbo de data e hora.

   vm_type

Especifica o tipo de hipervisor em que se executa o teste de Recuperação garantida. Os tipos de hipervisores válidos são Hyper-V , ESX e AHV.

vm_server

Especifica o endereço do servidor do hypervisor. O endereço é o nome do host ou o endereço IP.

vm_svr_username

Especifica o nome de usuário do hypervisor.

vm_svr_password

Especifica a senha do hypervisor. A senha é criptografada usando o utilitário de criptografia d2dutil.

vm_svr_protocol

Especifica o protocolo do hipervisor quando você executa uma recuperação garantida no vCenter/ESX(i) ou no AHV.

vm_svr_port

Especifica a porta do hipervisor quando você executa uma recuperação garantida no vCenter/ESX(i) ou no AHV.

vm_sub_server

Especifica o nome do servidor ESX ao executar a recuperação garantida no vCenter ou especifica o nome do agrupamento do Prism Element ao executar a recuperação garantida no Prism Central.

vm_datastore

Especifica o local de armazenamento da VM usado pelo teste de Recuperação garantida. O local é o repositório de dados no servidor ESX(i) ao se executar o teste de Recuperação garantida no vCenter/ESXI(i). O local deve ser um caminho local no servidor Hyper-V quando você executa a recuperação garantida no Hyper-V. O local é storage_container no agrupamento do AHV quando você executa a recuperação garantida no AHV.

vm_resource_pool

Especifica o nome do pool de recursos quando você executa uma recuperação garantida no vCenter/ESXI(i)

tempo limite

Especifica, durante a reinicialização, o tempo da tarefa de recuperação garantida até a VM estar pronta para uso. A unidade de tempo está em segundos.

vm_memory

Especifica o tamanho da memória da VM. O tamanho da unidade é expresso em MB, em múltiplos de 4.

vm_cpu_count

Especifica o número de CPU da VM.

run_after_backup

Especifica que a tarefa de Recuperação garantida seja executada uma vez ou todas as vezes para a tarefa de backup que está definida pelo parâmetro backup_job_name. A tarefa de Recuperação garantida é executada imediatamente para a tarefa de backup especificada quando definida como **não**, e é executada todas as vezes após a conclusão da tarefa de backup especificada quando definida como **sim**.

Padrão: no

backup_job_name

Especifica o nome da tarefa de backup de nós para executar a tarefa de Recuperação garantida.

storage_type

Especifica o tipo de armazenamento para a sessão cujo backup foi feito. Os tipos válidos de armazenamento são cifs, nfs e rps.

storage_location

Especifica o local do NFS ou CIFS.

storage_username

Especifica o nome de usuário para o local do CIFS.

storage_password

Especifica a senha para o local do CIFS. A senha é criptografada usando o utilitário de criptografia d2dutil.

rps_protocol

Especifica o protocolo do servidor de ponto de recuperação quando se executa a tarefa de Recuperação garantida para as sessões no servidor de ponto de recuperação.

rps_hostname

Especifica o nome do host do servidor do ponto de recuperação. O endereço pode ser o nome do host ou o endereço IP.

rps_username

Especifica o nome de usuário do servidor do ponto de recuperação.

rps_password

Especifica a senha do servidor do ponto de recuperação. A senha é criptografada usando o utilitário de criptografia d2dutil.

rps_port

Especifica a porta do servidor do ponto de recuperação.

Valor padrão: 8014.

rps_datastore

Especifica o nome do repositório de dados do servidor do ponto de recuperação.

encryption_password

Especifica a senha da sessão criptografada. A senha é criptografada usando o utilitário de criptografia d2dutil.

node_name_list

Especifica o(s) nome(s) do(s) nó(s) em que o teste de Recuperação garantida é executado. Os nomes são separados usando ";". Se um nome não for especificado ou for deixado em branco, todos os nós com o mesmo nome de tarefa de backup ou que estejam no mesmo local executarão o teste de Recuperação garantida.

recovery_point_date_filter

Especifica a data do ponto de recuperação. O teste de Recuperação garantida é executado para o último ponto de recuperação antes da data especificada. Se a data não for especificada ou for deixada em branco, a sessão cujo backup foi feito mais recentemente executará o teste de Recuperação garantida.

gateway_vm_network

Especifica a rede da VM para o servidor de gateway. A VM e o servidor de backup estão na mesma rede.

gateway_guest_network

Especifica o tipo de endereço IP da rede para o servidor de gateway. A rede é dhcp ou estática.

gateway_guest_ip

Especifica o endereço IP do servidor de gateway se você fornecer o IP estático.

gateway_guest_netmask

Especifica a máscara de rede do servidor de gateway se você fornecer o IP estático.

gateway_guest_gateway

Especifica o gateway para o servidor de gateway se você especificar o IP estático.

script_post_job_server

(Opcional) Especifica o script a ser executado após a tarefa ser concluída no servidor de backup.

script_ready_to_use

(Opcional) Especifica o script a ser executado quando o computador de destino está pronto para uso na VM da Recuperação garantida.

run_script_ready_to_use_timeout

Especifica o tempo para execução do script pronto para uso especificado pelo script_ready_to_use. A unidade de tempo está em segundos.

Observação: parâmetros para as informações relacionadas à sessão, incluindo s*torage_type, storage_location, storage_username, storage_password, rps_protocol, rps_hostname, rps_username, rps_password, rps_port, and rps_datastore* só são necessários quando *backup_job_name* não é especificado.

5. Clique em **Salvar** e feche o modelo de configuração.

   O modelo de configuração foi criado com êxito.

Modificar o arquivo e o modelo de configuração

Se você já tiver o arquivo de modelo de configuração, é possível modificar o arquivo e executar o teste de Recuperação garantida com uma configuração diferente. Não é necessário criar outro modelo de configuração. Ao enviar a tarefa, uma nova tarefa é adicionada à interface da web. É possível exibir os logs de atividades na interface da web.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o modelo de configuração a partir do local em que você salvou o arquivo e modifique os parâmetros de acordo com as suas necessidades.
3. Clique em **Salvar** e feche o modelo de configuração.
4. Clique em Salvar e feche o arquivo de configuração global.

O modelo de configuração foi modificado com êxito.

Enviar uma tarefa usando o utilitário d2dar

Você pode usar o comando d2dar para executar o teste de Recuperação garantida para as sessões armazenadas em backup. Após o envio, é possível exibir a tarefa pela interface da web. Durante o processo de Recuperação garantida, se qualquer requisito não for atendido, a linha de comando exibirá um erro. Também é possível exibir o log de atividades na interface da web.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Envie a tarefa de Recuperação garantida por meio do seguinte comando:

   #./d2dar --template=cfg_file_path

Como montar o ponto de recuperação

A opção Montar ponto de recuperação pode compartilhar arquivos em um Ponto de recuperação por meio de NFS ou WebDAV, e é possível acessar esses arquivos montando o local no servidor Linux.

Execute estas tarefas para Montar ponto de recuperação:

- Verificar os pré-requisitos
- Especifique o Ponto de recuperação para Montar ponto de recuperação
- Especifique as configurações para Montar ponto de recuperação
- Criar e executar a tarefa Montar ponto de recuperação
- Montar compartilhamento de NFS ou de WebDAV no servidor Linux

Verificar os pré-requisitos

Considere os pré-requisitos a seguir antes de montar o ponto de recuperação:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver.
- Se você deseja montar o ponto de recuperação por WebDAV, certifique-se de que o pacote davfs2 tenha sido instalado no servidor Linux.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais suportados.

Especifique o Ponto de recuperação para Montar ponto de recuperação

Sempre que você executa um backup, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no Assistente de restauração de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

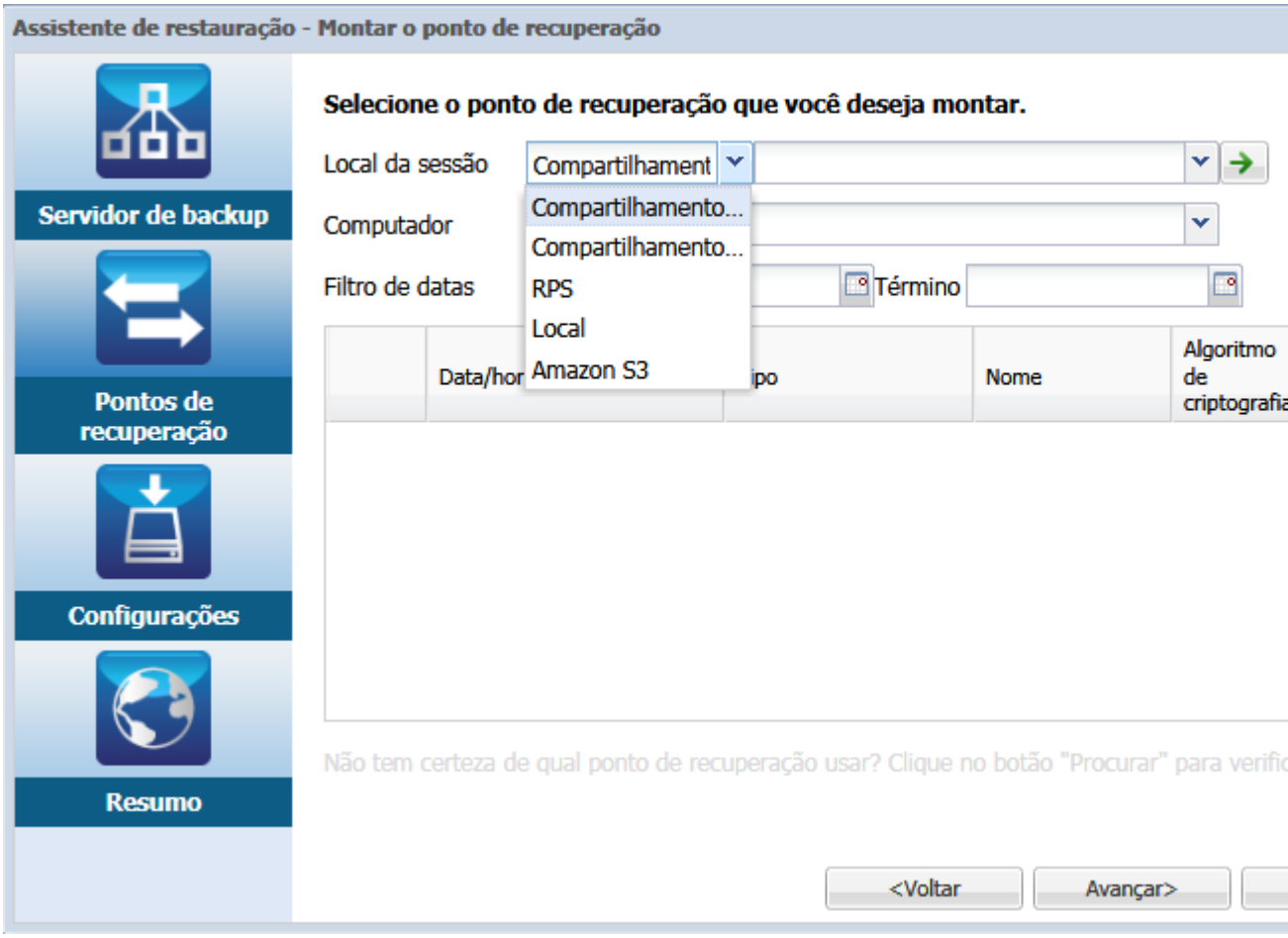
Siga estas etapas:

1. Abra a interface da web do agente do Arcserve UDP (Linux).
2. Clique em **Restaurar** no menu do **Assistente** e selecione **Montar ponto de recuperação**.

   Assistente de restauração – Montar ponto de recuperação é aberta.

   É possível ver o servidor de backup na página Servidor de backup do Assistente de restauração. Não é possível selecionar nenhuma opção na lista suspensa **Servidor de backup**.
3. Clique em **Avançar**.

   A página **Pontos de recuperação** do **Assistente de restauração** é exibida.



4. Selecione um **compartilhamento CIFS/compartilhamento NFS/servidor RPS/Local** na lista suspensa Local da sessão.
5. Siga uma das seguintes etapas, dependendo do local da sessão:

   Para compartilhamento de CIFS/compartilhamento de NFS/Local

   Especifique o caminho completo do compartilhamento CIFS/-compartilhamento NFS/Local e clique em **Conectar**.

   Todas as máquinas são listadas na lista suspensa **Computador**.

   Observação: se você selecionar a opção Compartilhamento CIFS, especifique o nome de usuário e a senha.

   Para o servidor RPS

   a. Selecione o servidor RPS e clique em **Adicionar**.

      A caixa de diálogo Informações do **servidor de ponto de recuperação** abre.

   b. Forneça os detalhes do RPS e clique no botão **Carregar**.

c. Selecione o repositório de dados na lista suspensa e clique em **Sim**.

   A caixa de diálogo Informações do servidor de ponto de recuperação fecha e você vê o assistente.

d. Clique em **Conectar**.

   Todas as máquinas são listadas na lista suspensa Computador.

e. Selecione o computador na lista suspensa.

   Todos os pontos de recuperação da máquina selecionada são exibidos abaixo da opção **Filtro de datas**.

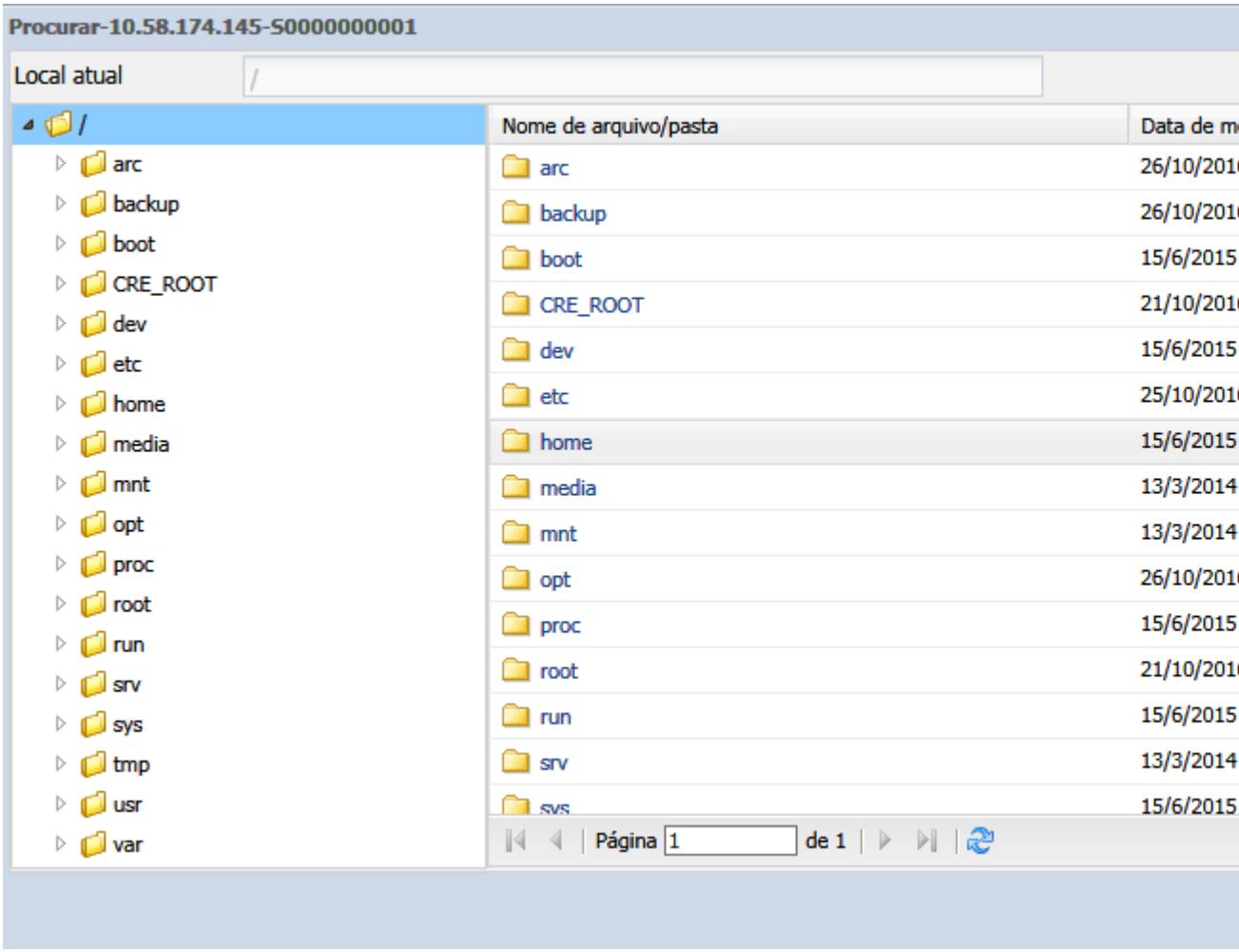
6. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

   Padrão: últimas duas semanas.

   Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

7. Clique em Procurar para exibir o ponto de recuperação.

   A caixa de diálogo **Procurar-<nome do nó>-<número da sessão>** é aberta.



Observação: se você tentar localizar um arquivo ou pasta usando o campo **Pesquisar**, certifique-se de que tenha selecionado a pasta de nível mais alto na hierarquia. A pesquisa é conduzida em todas as pastas filhas da pasta selecionada.

8. Clique em **OK**.

   A caixa de diálogo **Procurar-<nome do nó>>-<-<número da sessão>** > é fechada e você retorna à página Pontos de recuperação.

9. Clique em **Avançar**.

   A opção **Configurações** para as páginas Montar ponto de recuperação é aberta.

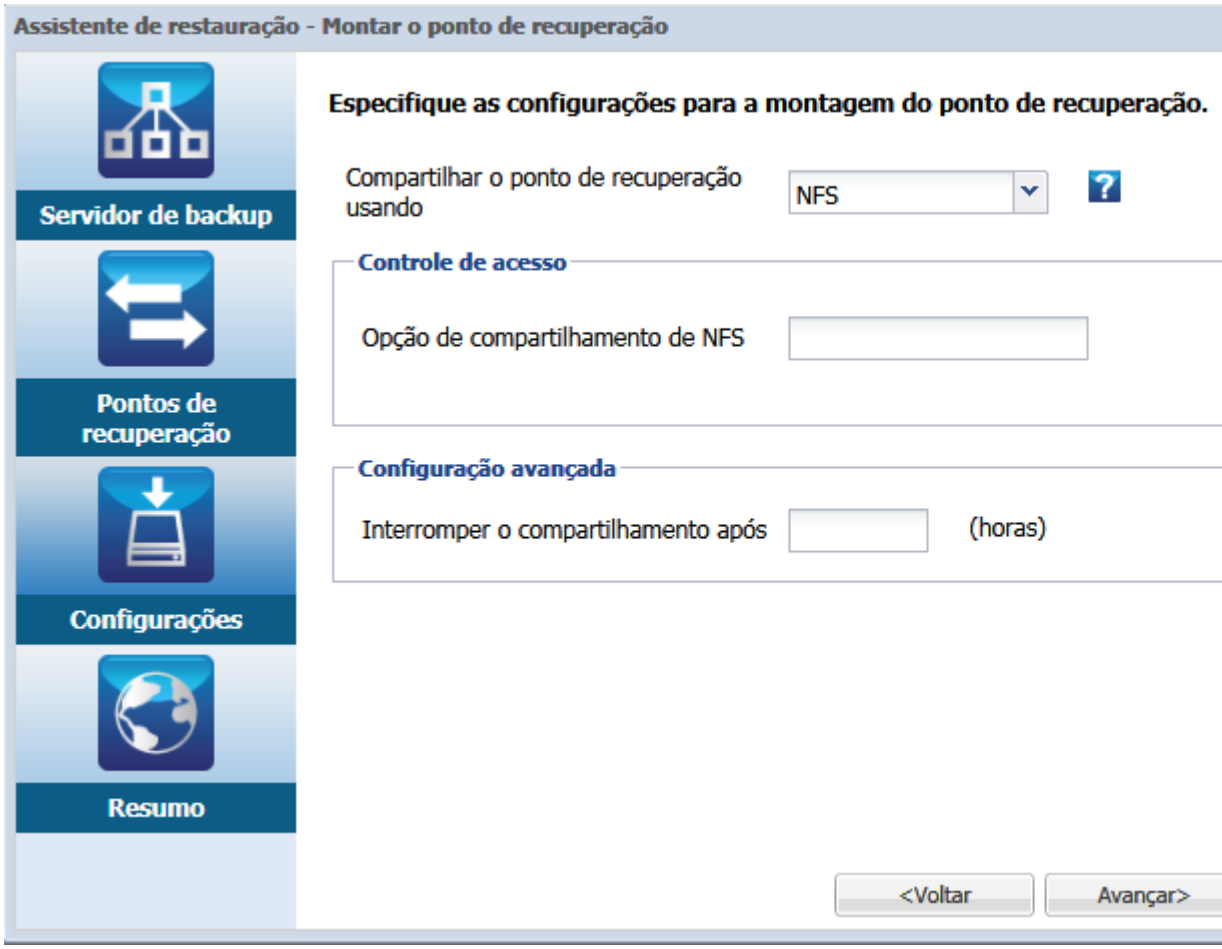
Especificar as configurações para Montar ponto de recuperação

Especifique as configurações para Montar ponto de recuperação para escolher o método de compartilhamento apropriado.

Siga estas etapas:

1. Para montar o ponto de recuperação por NFS, siga estas etapas:
   a. Selecione **NFS** na lista suspensa de método de compartilhamento.

      Os arquivos no ponto de recuperação serão compartilhados via NFS. E é possível montar o compartilhamento de NFS em qualquer máquina que possa acessar o servidor de backup Linux.



   b. (Opcional) Digite **Opção de compartilhamento de NFS** de acordo com sua necessidade.

Consulte a página principal para exportações, opções da Candidate e formato válido. Deixe em branco se você não precisar de controle de acesso.

c. Digite **Hora** para a hora que o compartilhamento será interrompido após a(s) hora(s) especificada(s).

Se você digitar 0 nesse campo, o compartilhamento poderá ser acessado continuamente.

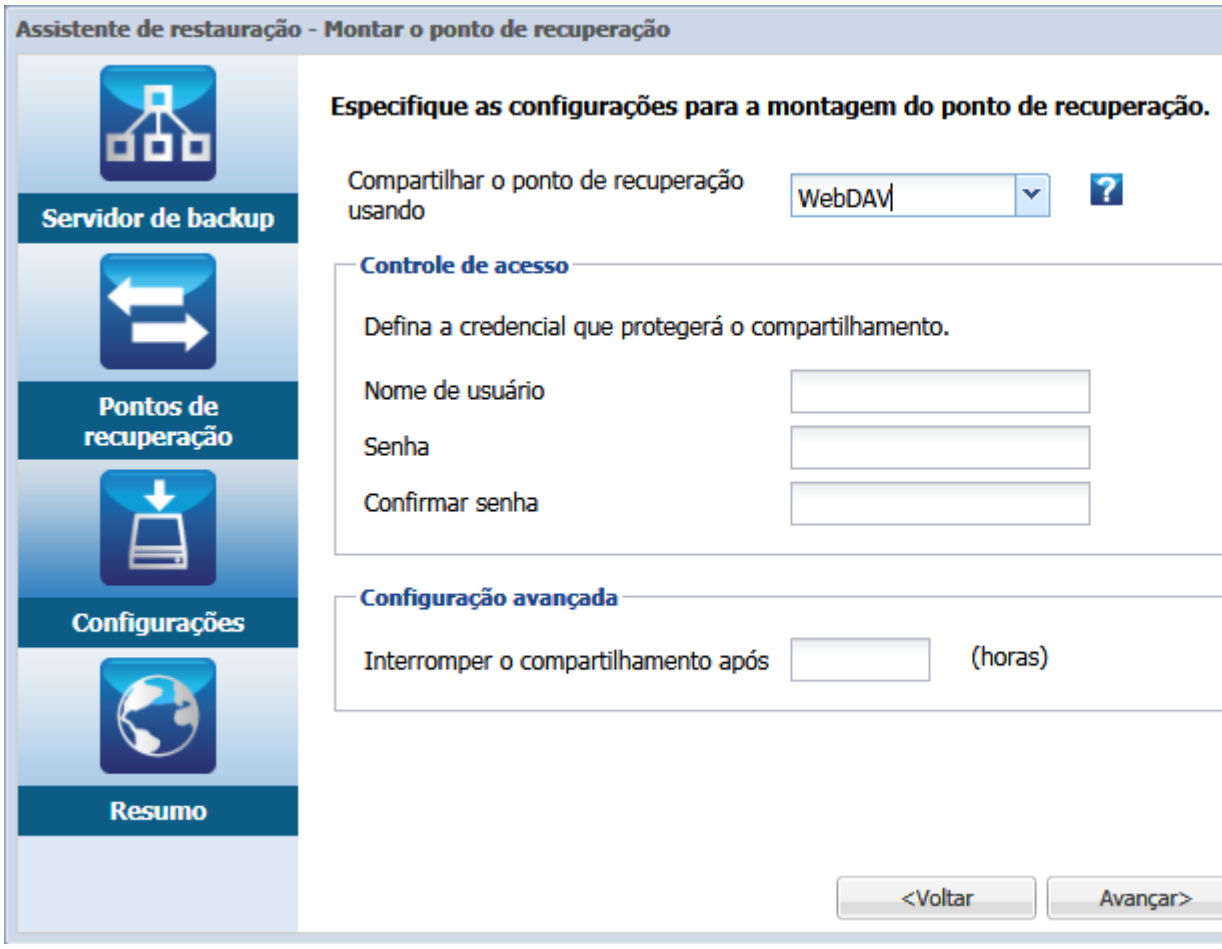
d. Clique em **Avançar**.

A página de resumo da tarefa Montar ponto de recuperação é aberta.

2. Para montar o ponto de recuperação por WebDAV, siga estas etapas:

a. Selecione **WebDAV** na lista suspensa de método de compartilhamento.

Os arquivos no ponto de recuperação serão compartilhados via WebDAV. E é possível montar o compartilhamento por WebDAV usando mount.davfs. Esse é o método recomendado quando é preciso acessar o compartilhamento pela internet.



b. Digite o **Nome de usuário**, a **Senha** e digite novamente a senha em **Confirme sua senha** para o controle de acesso.

   Lembre-se do nome de usuário e da senha, pois eles serão necessários para acessar o ponto de recuperação montado.

c. Digite **Hora** para a hora que o compartilhamento será interrompido após a(s) hora(s) especificada(s).

   Se você digitar 0 nesse campo, o compartilhamento poderá ser acessado continuamente.

   Se chegar a hora especificada, o ponto de recuperação montado não poderá ser acessado.

d. Clique em **Avançar**.

   A página Resumo da tarefa Montar ponto de recuperação é aberta.

Criar e executar a tarefa Montar ponto de recuperação

É possível criar e executar a tarefa Montar ponto de recuperação para acessar os arquivos no Ponto de recuperação especificado. Verifique as informações de configuração antes de enviar a tarefa. Se necessário, é possível voltar e alterar as configurações no assistente.

Siga estas etapas:

1. Verifique os detalhes de Montar ponto de recuperação na página **Resumo**.
2. (Opcional) Clique em **Voltar** para modificar as informações que você digitou em qualquer página do Assistente de restauração.
3. Digite um nome da tarefa e clique em **Enviar**.

   O campo **Nome da tarefa** tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

   O **Assistente de restauração** é fechado. É possível ver o status da tarefa na guia **Status da tarefa**.

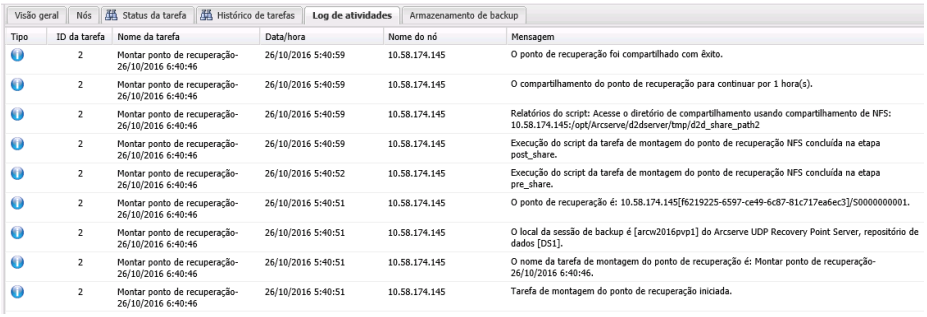
   A tarefa Montar ponto de recuperação é criada e executada com êxito.

Montar compartilhamento de NFS ou de WebDAV no servidor Linux

É possível acessar o ponto de recuperação montado após a **Fase da tarefa** na guia **Status da tarefa** ser **Ponto de recuperação de compartilhamento**.

Siga estas etapas:

1. Obtenha a **ID da tarefa/nome da tarefa** da tarefa Montar ponto de recuperação na guia **Status da tarefa**.
2. Filtre os logs de atividades da tarefa Montar ponto de recuperação pela **ID da tarefa/nome de tarefa** na página **Log de atividades** usando as ferramentas de **Filtro**.



3. Tenha o diretório compartilhado para o ponto de recuperação montado exibido no log de atividades.

   Formato do diretório durante a montagem por meio de NFS:

   < d2dserver >:/opt/Arcserve/d2dserver/tmp/d2d_share_path<jobid>

   É possível acessar os arquivos no ponto de recuperação montando o diretório.

   Exemplo:

   mount *< d2dserver >:/opt/Arcserve/d2dserver/tmp/d2d_share_path<jobid> /mnt*

   Formato do diretório durante a montagem por meio de WebDAV:

   https://<d2dserver>:8014/share/<nome_de usuário>/

   É possível acessar os arquivos no ponto de recuperação com o navegador da web ou montando o diretório.

   Exemplo:

   mount.dafs https://<d2dserver>:8014/share/<nome_de usuário>/ /mnt

4. Digite o nome de usuário e a senha fornecida ao enviar a tarefa Montar ponto de recuperação.

Instalar o pacote davfs no servidor Linux

É possível instalar o pacote davfs no servidor Linux.

- Para o Red Hat Linux, o Linux CentOS ou o Oracle Linux

  Siga estas etapas:

  1. Obtenha o Extra Packages for Enterprise Linux (EPEL) para o servidor Linux com a versão correspondente do http://-fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F
  2. Copie o pacote EPEL baixado para o servidor Linux de destino.
  3. Instale o pacote EPEL pelo comando conforme abaixo

     # yum install <caminho_do_pacote>/epel-release-<informações_da_versão>. rpm
  4. Instale o pacote davfs2 pelo comando conforme a seguir.

     # yum install davfs2

- Para SuSE Linux 12 SP1

  Siga estas etapas:

  1. Efetue logon no servidor Linux.
  2. Instale o pacote davfs2 pelo comando conforme a seguir.

     # zypper addrepo

     # zypper refresh

     # zypper install davfs2

  Para obter mais informações, consulte o link.

Como ativar o suporte ao kernel mais recente do Ubuntu

O Ubuntu atualiza seu kernel regularmente, o que resulta na desatualização dos drivers enviados com a release. Embora a desativação do processo automático de atualização do kernel do sistema Ubuntu ajude, a Arcserve também oferece suporte aos kernels atualizados, quando necessário.

Importante: apesar de nossos esforços para oferecer suporte ao kernel mais recente do Ubuntu, alterações significativas no kernel ainda poderão atrasar ou cancelar os drivers correspondentes.

Como gerente de armazenamento, você pode analisar os cenários abaixo para ativar o uso do Agente do Arcserve UDP (Linux) com o kernel mais recente do Ubuntu:

- Se seu servidor do Agente do Arcserve UDP (Linux) tiver uma conexão de internet ativa, os drivers atualizados serão baixados e implantados de maneira autônoma. Você pode usar o software sem esforços adicionais.
- Se seu servidor do Agente do Arcserve UDP (Linux) não tiver acesso à internet, você poderá fazer download e implantar o pacote de driver atualizado manualmente.
- Se você tiver vários servidores do Agente do Arcserve UDP (Linux), poderá implantar o pacote de driver atualizado em um servidor e, então, configurar o outro servidor para ser usado como um servidor de armazenamento temporário.

Execute as etapas a seguir para implantar o pacote de driver atualizado:

- Verificar os pré-requisitos
- Implantar o pacote de driver atualizado do Ubuntu manualmente
- (Opcional) Usando o servidor de armazenamento temporário para atualizar drivers
- (Opcional) Configurando o proxy HTTP

Verificar os pré-requisitos

Considere os seguintes pré-requisitos:

- Você tem as credenciais de logon raiz disponíveis para efetuar logon no servidor de backup.
- Você tem o curl ou o wget instalados no servidor de backup.
- Você tem o gpg instalado no servidor de backup.

Implantar o pacote de driver atualizado do Ubuntu manualmente

Se seu servidor do Agente do Arcserve UDP (Linux) não tiver acesso à internet, você ainda poderá atualizar os drivers fazendo download e implantando os drivers manualmente.

Siga estas etapas:

1. Faça download do pacote de driver e da assinatura. Consulte o suporte da Arcserve para obter o URL.

   Observação: coloque o arquivo de assinatura obtido por download e o pacote de driver no formato *.tar.gz no local da pasta de destino. Não extraia os arquivos.

2. Efetue logon no servidor de backup como usuário raiz.
3. Navegue até o local onde está o pacote obtido por download e inicie a implantação usando os seguintes comandos:

   # source /opt/Arcserve/d2dserver/bin/setenv

   # /opt/Arcserve/d2dserver/bin/d2dupgradetool deploy <pasta contendo o pacote baixado>

   O pacote de driver atualizado é implantado com êxito.

(Opcional) Usando o servidor de armazenamento temporário para atualizar drivers

Se você tiver vários servidores do Agente do Arcserve UDP (Linux) que precisam oferecer suporte ao kernel mais recente do Ubuntu, poderá configurar um deles para funcionar como servidor de armazenamento temporário. Verifique se o servidor de armazenamento temporário já está com o driver atualizado implantado usando a conexão de internet ativa ou siga as instruções em Implantar o pacote de driver atualizado do Ubuntu manualmente. Você pode configurar cada servidor de backup que precisa do pacote de driver atualizado do Ubuntu.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra e edite o arquivo de configuração:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg

3. Edite os seguintes itens de configuração:

   scheme=<http ou https>

   host=<endereço do servidor de armazenamento temporário>

   port=<porta do servidor do agente, normalmente 8014>

   A atualização automática do pacote de driver é configurada com êxito.

(Opcional) Usando o servidor de armazenamento temporário para atualizar drivers

Você pode configurar o proxy do Agente do Arcserve UDP (Linux) para acessar a conexão de internet.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra e edite o arquivo de configuração:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg

3. Edite os seguintes itens de configuração:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg

   http_proxy=<endereço do proxy>

   proxy_user=<nome de usuário>

   proxy_password=<senha>

   O proxy foi configurado com êxito.

Como desativar o bit SUID durante a execução da tarefa de restauração de arquivo

Ao executar a tarefa de restauração de arquivo usando credenciais do usuário sudo (não raiz) do nó de destino, o bit SUID é definido para o binário d2dtar para potencializar seu uso. Esse binário d2dtar é executado no nó de destino durante a tarefa de restauração de arquivo. Em alguns ambientes, o uso do bit SUID é desativado para assegurar a segurança dos dados. Esta seção fornece informações sobre como desativar o bit SUID para o binário d2dtar.

Esta seção contém os seguintes tópicos:

Verificar os pré-requisitos

Considere os seguintes pré-requisitos:

- Você tem as credenciais de logon raiz para efetuar logon no servidor de backup Linux.
- Você tem as credenciais de logon raiz do nó de destino para modificar o arquivo *sudoers*.

Definir configurações no servidor de backup Linux

Esta seção fornece informações sobre como definir as configurações no servidor de backup Linux.

Siga estas etapas:

1. Efetue logon no servidor de backup Linux usando credenciais raiz.
2. Navegue até o arquivo */opt/Arcserve/d2dserver/configfiles/server.env* e adicione a linha a seguir:

   "export FLR_DISABLE_SUID=1"

   Observação: se o arquivo *server.env* não existir em */opt/Arcserve/d2dserver/configfiles*, crie o arquivo *server.env* e adicione a linha acima ao arquivo *server.env*.
3. Para reiniciar o d2dserver, execute o seguinte comando:

   # /opt/Arcserve/d2dserver/bin/d2dserver restart

Configurar o sudo para autorizar o binário d2dtar no nó de destino

Esta seção fornece informações sobre como configurar o sudo para autorizar o binário d2dtar no nó de destino.

Siga estas etapas:

1. Efetue logon no nó de destino usando credenciais raiz.
2. Para editar o arquivo de configuração, abra o arquivo */etc/sudoer* usando o comando *visudo*.
3. Adicione a linha a seguir:

   <sudo-user> ALL=(ALL) NOPASSWD: /home/<sudo-user>/.d2-drestorefile/d2dtar.64,/tmp/d2dtar.64

   Exemplo: se udplinux for um usuário sudo, adicione a seguinte linha ao arquivo /etc/sudoers:

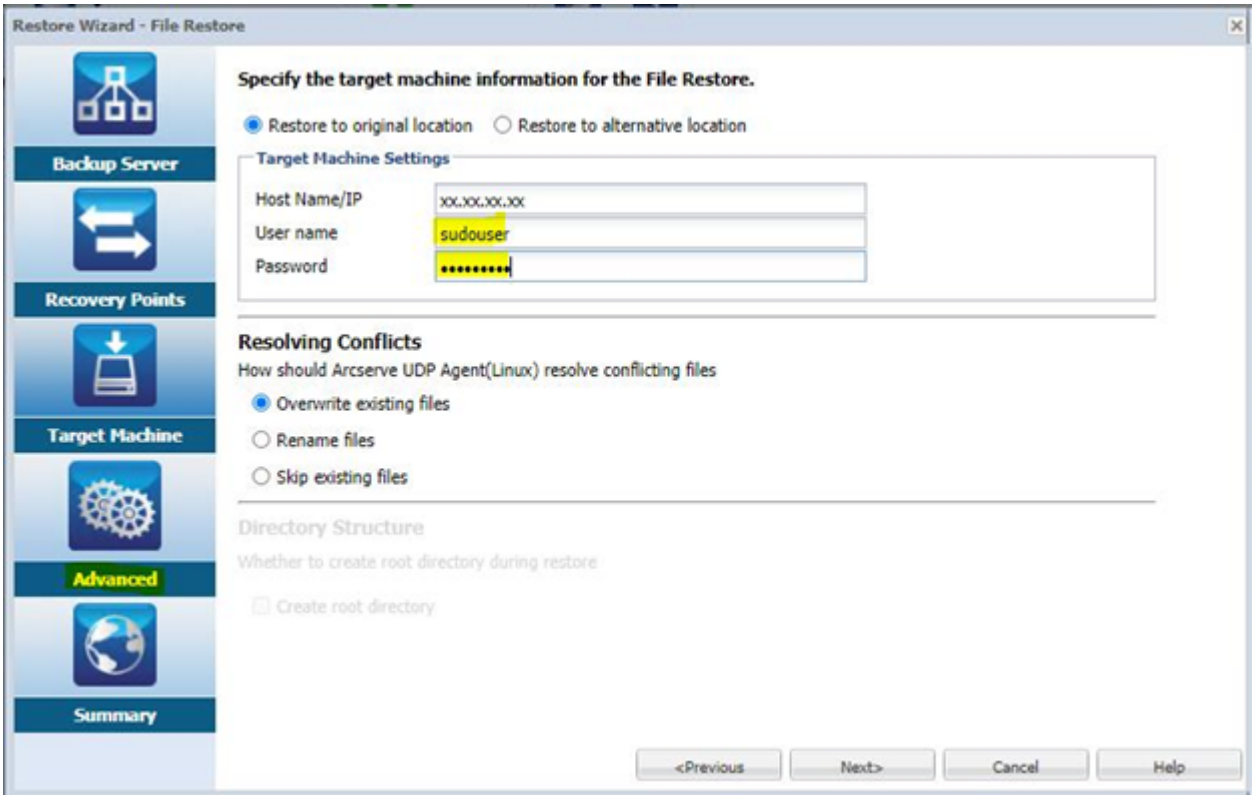
   udplinux ALL=(ALL) NOPASSWD: /ho-me/udplinux/.d2drestorefile/d2dtar.64,/tmp/d2dtar.64

Executar a tarefa de restauração de arquivo usando as credenciais de usuário sudo do nó de destino

Esta seção fornece informações sobre como executar a tarefa Restaurar arquivo usando credenciais de usuário sudo.

Siga estas etapas:

1. Abra o assistente de restauração de arquivos e preencha os detalhes, conforme necessário.
2. Na página Avançado, em Configurações do computador de destino, forneça as credenciais do usuário sudo e execute a tarefa Restaurar arquivo.



O bit SUID é desativado para o binário d2dtar no nó de destino durante a execução da tarefa Restaurar arquivo.

Capítulo 6: Solução de problemas

Esta seção contém os seguintes tópicos:

Falha na instalação do Agente do Arcserve UDP (Linux) nos servidores com suporte

Válido no CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11 SP3/SP4 e Oracle Linux Server 6.x

Sintoma

Quando instalo o Agente do Arcserve UDP (Linux), a instalação apresenta falha com as seguintes mensagens de aviso do Linux:

```
mkisofs                 Tratar a imagem LiveCD

mount.nfs              Montar compartilhamento NFS

o sistema de arquivos como destino do backup e origem da res-
tauração

mount.cifs              Montar o sistema de compartilhamento
de arquivos CIFS como destino do backup e origem da res-
tauração

Os processos a seguir precisam estar em execução

Processos inativos                              Função afe-
tada

rpc.statd                A função de bloqueio de arquivos
NFS não funciona
```

Solução

No início da instalação, o Agente do Arcserve UDP (Linux) verifica se o sistema operacional Linux atende ao requisito do servidor de backup. Se o sistema operacional Linux não atender aos requisitos mínimos, o Agente do Arcserve UDP (Linux) exibirá uma mensagem de aviso para informá-lo sobre esse problema. A mensagem inclui a lista de todos os pacotes que são necessários para o servidor de backup.

Para resolver esse problema de instalação do Agente do Arcserve UDP (Linux), siga estas etapas:

1. Instale os seguintes pacotes usando o comando *yum*:
   - genisoimage
   - nfs-utils
   - cifs-utils
2. Execute estes dois comandos:

   ```
   service rpcbind start
   ```

```
service nfs start
```

3. Execute o seguinte comando para verificar se *rpc.statd* está em execução:

   ```
   ps -ef|grep rpc.statd
   ```

4. Reinstale o Agente do Arcserve UDP (Linux).

   O Agente do Arcserve UDP (Linux) é instalado com êxito.

Exibição de erro de tempo limite da operação no Agente do Arcserve UDP (Linux)

Válido no CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11 SP3/SP4 e Oracle Linux Server 6.x

Sintoma

Recebo a seguinte mensagem de erro:

O tempo limite da operação foi atingido. A quantidade máxima de tempo para concluir a operação foi excedida. Tente novamente mais tarde.

Recebo com frequência esta mensagem quando executo uma restauração em nível de arquivo e procuro por pontos de recuperação que têm mais de 1000 pontos de recuperação incremental.

Solução

O valor do tempo limite padrão é 3 minutos. É possível solucionar o problema, aumentando o valor do tempo limite.

Para aumentar o valor de tempo limite, execute as seguintes etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Adicione a seguinte variável de ambiente do sistema:

   `D2D_WEBSVR_TIMEOUT`

   O valor da variável de ambiente é um número. O número deve ser superior a 3. A unidade do valor é o minuto.
3. Reinicie o servidor de backup.

   O valor do tempo limite é aumentado com êxito.

Há falha em todas as tarefas programadas quando a hora do sistema é alterada para um valor já transmitido

Válido no CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11 SP3/SP4 e Oracle Linux Server 6.x

Sintoma

Ao alterar a hora do sistema para um valor passado, todas as minhas tarefas programadas são afetadas. As tarefas programadas não funcionam depois de alterar a hora do sistema para uma hora anterior.

Solução

Depois de alterar a hora do sistema, reinicie o serviço do BACKUP.

Siga estas etapas para reiniciar o serviço do BACKUP:

1. Efetue logon no servidor de backup como usuário raiz.
2. Vá até a pasta bin

   ```
   /opt/Arcserve/d2dserver/bin/
   ```

3. Reinicie o servidor de backup usando o seguinte comando:

   ```
   d2dserver restart
   ```

   O servidor de backup é reiniciado.

   Todas as tarefas programadas são executadas conforme a programação.

Falha do Agente do Arcserve UDP (Linux) ao montar dispositivos RAID do software Linux

Válido no CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11 SP3/SP4 e Oracle Linux Server 6.x

Sintoma

Às vezes, o processo de BMR falha ao montar os dispositivos RAID do software Linux após o computador de destino reiniciar.

Solução

Para resolver este problema, reinicie o computador de destino.

Agente do Arcserve UDP (Linux) Falha ao fazer download e implantar os drivers atualizados do Ubuntu no SLES 11 e no RHEL 6

Válido em algumas versões desatualizadas do SUSE Linux Enterprise Server (SLES) 11 e do Red Hat Enterprise Linux (RHEL) 6

Sintoma

Quando tento fazer backup do nó do Ubuntu que tem a versão atualizada do kernel, ocorre uma falha na tarefa de backup, e a mensagem no log de atividades refere-se a uma falha no download e na implantação dos drivers do Ubuntu.

Solução

Atualize os pacotes do sistema e verifique se você tem a versão mais recente dos utilitários curl ou wget.

Siga estas etapas:

1. Reinicie a máquina de destino.
2. Execute o seguinte comando:

   No SUSE: zypper update wget curl

   No RHEL: yum update wget curl
3. Execute novamente a tarefa de backup que falhou no nó do Ubuntu.

O driver do Ubuntu é atualizado com êxito.

A PVM exibe uma tela preta na janela do cliente de VNC ao inicializar usando um Live CD

Válido para PVM no Oracle VM Server

Sintoma

Em um Oracle VM Server, quando inicializo a PVM (Paravirtual Machine - Máquina Paravirtual) usando um Live CD, vejo uma tela preta na janela do cliente de VNC (Virtual Network Computing - Computação em Rede Virtual).

Solução

Para resolver esse problema, efetue logon no console do Live CD a partir do back-end.

Siga estas etapas:

1. Inicie a VM usando um Live CD.
2. Anote a ID da VM que você pode acessar a partir do Oracle VM Manager.

3. Efetue logon no Oracle VM Server em que a VM está em execução usando o SSH (Secure Shell).
4. Execute o comando *xm console $ID*, conforme mostrado no seguinte diagrama:

5. (Opcional) Pressione Enter quando solicitado a confirmar a operação.
6. O console da PVM Xen inicializada com o Live CD é aberto.
7. Configure a rede.
8. Saia do console pressionando ctrl+] ou ctrl+5.

   O problema foi resolvido.

Ocorre uma falha na tarefa de backup ao coletar informações relacionadas à BMR ou na tarefa de BMR ao criar um layout de disco

Válido para o Oracle VM Server para HVM com volume LVM

Sintoma

Ao executar uma tarefa de backup para uma HVM com volumes LVM em um Oracle VM Server, há falha na tarefa de backup ao coletar as informações relacionadas à BMR. Além disso, quando executo uma tarefa de BMR para uma HVM com volumes LVM em um Oracle VM Server, há falha na tarefa de BMR ao criar o layout do disco.

Solução

Para resolver esse problema, desative os drivers PV para o nó de origem do backup.

Siga estas etapas:

1. Abra a janela Prompt de comando no nó de origem do backup e insira o seguinte comando:

   ```
   sfdisk –s
   ```

2. Verifique se o mesmo disco é exibido duas vezes no resultado.

   Por exemplo, xvdX e hdX são o mesmo disco. Verifique se ambos os discos são exibidos no resultado.

3. Se a resposta for afirmativa, execute estas etapas:

a. Adicione a seguinte linha ao arquivo */etc/modprobe.d/blacklist* no nó de origem do backup:

   ```
   blacklist xen_vbd
   ```

b. Reinicie o nó de origem do backup e execute novamente a tarefa de backup.

   A tarefa de backup é executada.

4. Caso isso não aconteça, entre em contato com a equipe de suporte da Arcserve.

   O problema foi resolvido.

Ocorre uma falha na tarefa de backup no RHEL7.0 como servidor de backup Linux e RPS no Windows Server 2019

Sintoma

Ocorre uma falha nas tarefas de backup ao instalar o RPS no Windows Server 2019 e o RHEL7.0 no agente do Linux, que usa o protocolo SMB1 para montar o CIFS, o que está desativado no Windows Server 2019.

Solução

Para executar a tarefa de backup com êxito, é necessário ativar o protocolo SMB1 no Windows Server 2019.

Siga estas etapas:

1. Para ativar o protocolo SMB1 no Windows Server 2019, execute o seguinte comando:

   Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

2. Reinicialize o servidor.

A tarefa de backup é executada com êxito.

Como ajustar uma sequência de inicialização de disco após uma tarefa de BMR em um Oracle VM Server

Válido no Oracle VM Server

Sintoma

Ao executar uma tarefa de BMR para um nó de destino em um Oracle VM Server, recebo a seguinte mensagem de aviso no log de atividades:

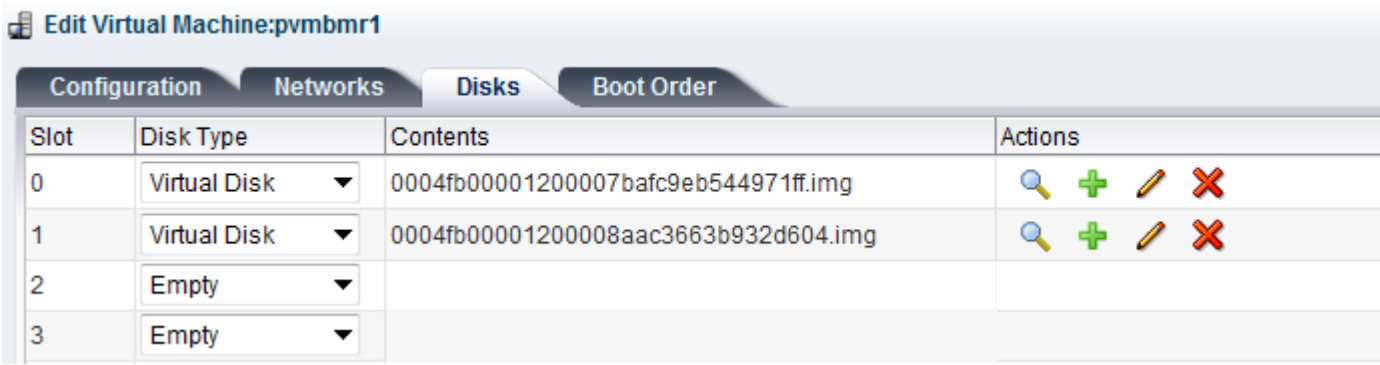
```
O volume de inicialização foi restaurado no disco /dev/xxx.
Ajuste a sequência de inicialização do disco em BIOS para
inicializar a partir de /dev/xxx.
```

Solução

Para evitar esse problema, troque a sequência de inicialização de disco do nó de destino da BMR.

Siga estas etapas:

1. Edite o nó de destino da BMR a partir do Oracle VM Manager e clique na guia Discos.

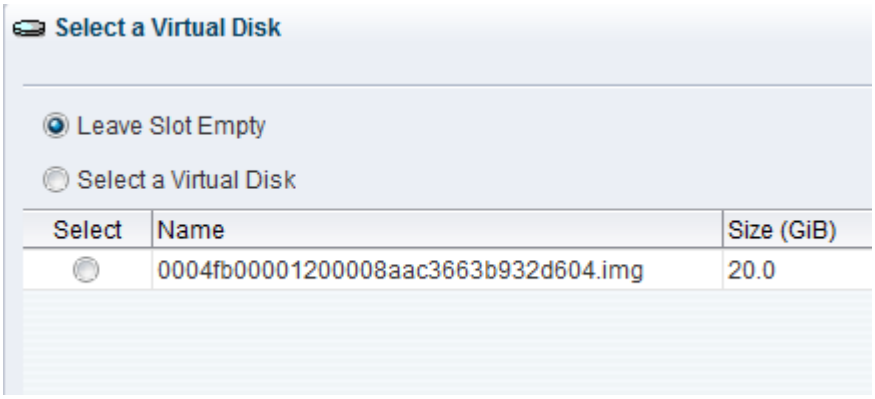


2. Selecione o disco do slot N como disco de inicialização.
3. Anote o nome do disco e o número do slot N.

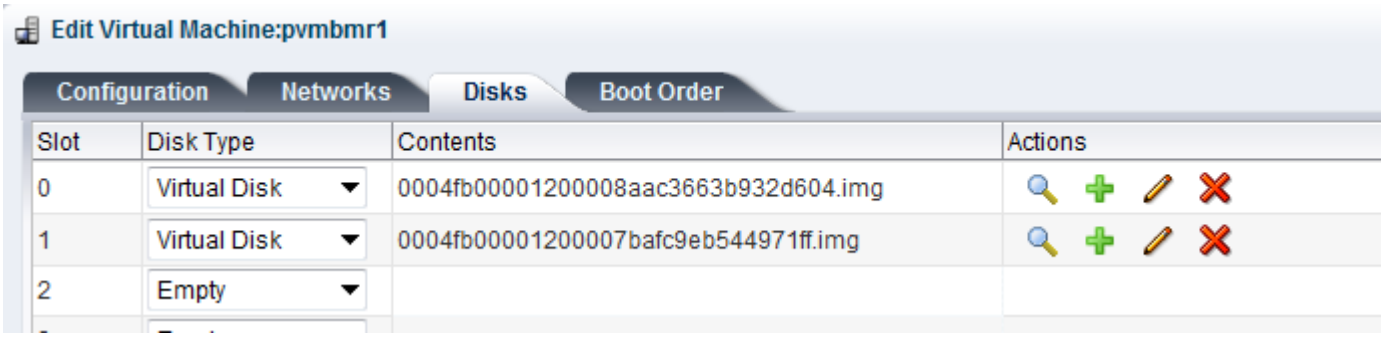
   Você usará o nome do disco e o número do slot em etapas posteriores.

4. Na coluna Ações, clique no botão Virtual Machine Disk.

5. Selecione a opção Leave Slot Empty e clique em Salvar.



6. Selecione o disco 0 do slot e anote o nome do disco.
7. Na coluna Ações, clique no botão Virtual Machine Disk.
8. Selecione a opção Leave Slot Empty e clique em Salvar.
9. Anexe a imagem do disco de inicialização selecionado ao slot 0, e a imagem do disco 0 do slot original ao slot N.



10. Inicialize o nó de destino da BMR.

    A sequência do disco de inicialização foi ajustada com êxito.

Como restaurar a versão anterior do servidor de backup

Válido no Red Hat Enterprise Linux (RHEL) 6.x e CentOS 6.x do servidor de backup

Sintoma

Tentei atualizar o servidor de backup, mas ocorreu um erro durante a atualização. O servidor de backup não está funcionando conforme o esperado. Agora, desejo restaurar a versão anterior do servidor de backup.

Solução

Ao fazer a atualização para uma nova release, o servidor de backup cria uma pasta de backup que contém todos os arquivos de configuração antigos e arquivos do banco de dados da versão instalada anteriormente. A pasta está no seguinte local:

```
/opt/Arcserve/d2dserver.bak
```

Siga estas etapas:

1. Desinstale o servidor de backup existente usando o seguinte comando:

   ```
   /opt/Arcserve/d2dserver/bin/d2duninstall
   ```

2. Instale a versão instalada anteriormente do servidor de backup.
3. Interrompa o servidor de backup usando o seguinte comando:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver stop
   ```

4. Copie os arquivos de configuração e arquivos do banco de dados antigos para a pasta d2dserver usando o seguinte comando:

   ```
   cp –Rpf /opt/Arcserve/d2dserver.bak/* /opt/Arcserve/d2d-
   server/
   ```

5. Inicie o servidor de backup usando o seguinte comando:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver start
   ```

   A versão instalada anteriormente do servidor de backup é restaurada com êxito.

Como fazer backup de instâncias do Debian 9.X EC2 na nuvem do AWS

Sintoma

Quando o backup é executado em instâncias do Debian 9.X EC2 na nuvem do AWS, a tarefa de backup falha sem exibir nenhum erro específico.

Solução

Quando as instâncias do Debian 9.X são criadas na nuvem do AWS e adicionadas à proteção, a ausência de módulos Perl poderá levar a erros. Para resolver esse problema, instale os pacotes usando os seguintes comandos:

sudo apt update

sudo apt install apt-file

sudo apt-file update

Falha na inicialização do nó de destino após a tarefa de migração da BMR ser executada para os nós do Debian 10.8 e 10.10

Sintoma

Quando a tarefa de migração da BMR é executada com o IVM, ocorre uma falha na inicialização do nó de destino e a seguinte mensagem de erro é exibida. Em seguida, o shell de resgate *initramfs* é inserido:

Erro de corrupção do sistema de arquivos raiz

Solução

Como solução alternativa, faça o seguinte:

1. Para verificar e reparar o volume de inicialização, execute o seguinte comando fsck:

   (initramfs) fsck -yf /dev/sdX

2. Para sair do shell de resgate *initramfs*, execute o seguinte comando:

   (initramfs) exit

O nó de destino é inicializado corretamente.

Falha na inicialização da VM para tarefa IVM/AR para o ESXi Server

Sintoma

Quando executo uma tarefa IVM/AR para o ESXi Server usando a sessão de backup sem agente e o nó de origem também está no ESXi Server, a VM não é inicializada no sistema com êxito.

Solução

A VM talvez precise de uma inserção de driver. É possível definir uma variável de ambiente para ativação.

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Abra o seguinte arquivo server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

3. Adicione o seguinte parâmetro ao arquivo server.env e salve o arquivo:

   ```
   export HBBU_VM_RESTORE_DISABLE=1
   ```

4. Reinicie o servidor de backup usando o seguinte comando:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

A VM oferece não é inicializada ao usar o adaptador de rede e1000e no nó do ESXi

Sintoma

Quando executo uma tarefa do IVM usando o adaptador de rede e1000e no nó do ESXi, a VM pode não ser inicializada no sistema com êxito.

Solução

É possível executar uma tarefa do IVM utilizando outras NICs disponíveis, mas não com a NIC e1000e.

O IVM para Hyper-V falha em inicializar corretamente para nós de origem do Debian 10.2/10.3/10.4/10.5

Sintoma

Se você selecionar a opção **Servidor com GUI** ao instalar qualquer um desses nós de origem, como Debian 10.2/10.3/10.4/10.5 no ESXI, e realizar a tarefa IVM para Hyper-V, o nó de destino gerado no Hyper-V não será devidamente inicializado. Embora os logs demonstrem êxito para a tarefa do IVM, ela falha em inicializar corretamente.

Solução

Depois que o nó de destino for criado na plataforma do Hyper-V e o status/os logs da tarefa “IVM para Hyper-V” mostrarem a conclusão bem-sucedida, reinicie o nó de destino manualmente. Após a reinicialização, o nó de destino abre a GUI esperada.

IVM para Hyper-V falha ao inicializar corretamente para o nó de origem do RHEL 8.0

Sintoma

Se você selecionar a opção **Servidor com GUI** ao instalar o RHEL 8.0 no ESXI e executar a tarefa IVM para Hyper-V, o nó de destino gerado no Hyper-V não será inicializado corretamente. Embora os logs demonstrem êxito para a tarefa IVM, ela falha ao inicializar.

Observação: esse problema está relacionado ao Redhat 8.0 na plataforma Hyper-V. Para obter mais informações sobre esse problema do Redhat 8.0, consulte o portal Redhat.

Ao contrário da série RHEL 7.x, os seguintes drivers não são instalados por padrão quando você seleciona a opção **Servidor com GUI** para instalação do RHEL 8.0:

- xorg-x11-drv-fbdev
- xorg-x11-drv-vesa
- xorg-x11-drv-vmware

Solução 1

Como solução alternativa, siga estas etapas:

1. Depois de instalar o nó de origem RHEL 8.0 no ESXI, instale os seguintes pacotes no nó:

   yum install xorg-x11-drv-fbdev xorg-x11-drv-vesa xorg-x11-drv-vmware -y
2. Execute um backup.
3. Use a mesma sessão de backup do RPS e execute a tarefa IVM no Hyper-V.

Solução 2

Use essa solução alternativa quando o backup não tiver sido executado após a instalação dos seguintes drivers:

- xorg-x11-drv-fbdev
- xorg-x11-drv-vesa
- xorg-x11-drv-vmware

Como solução alternativa, siga estas etapas:

1. Depois de executar o IVM para Hyper-V no RHEL 8.0 presente no ESXI ou depois de instalar o RHEL 8.0 no Hyper-V, na guia **Rede** do Hyper-V, obtenha o IP.

   Observação: nesse estado, a GUI não está disponível no nó do IVM.
2. Conecte a VM por meio de um aplicativo ssh (como putty) usando o IP.
3. Instale os seguintes pacotes no nó.

   yum install xorg-x11-drv-fbdev xorg-x11-drv-vesa xorg-x11-drv-vmware -y
4. Reinicialize o nó.

As tarefas d2drestorevm e d2dverify falham no Oracle VM Server

Válido no Oracle VM Server

Sintoma

Quando inicio as tarefas d2drestorevm e d2dverify em um Oracle VM Server, todas as tarefas falham. Recebo a seguinte mensagem de erro no log de atividades:

```
Falha ao importar a imagem ISO no hipervisor. Verifique o
console de gerenciamento do hipervisor ou o log de depuração
para obter informações mais detalhadas.
```

Solução

Verifique se o Oracle VM Server parou.

Siga estas etapas:

1. Efetue logon no console do Oracle VM Server e navegue até a guia Tarefas.
2. Localize todas as tarefas que estão com o status em andamento e cancele essas tarefas.
3. Inicie a tarefa d2drestorevm ou d2dverify novamente.

   Se a tarefa d2drestorevm ou d2dverify falhar novamente e exibir a mesma mensagem de erro, efetue logon no console do Oracle VM Server e verifique se há tarefas que exibem o status Em andamento. Se houver tarefas que exibem o status Em andamento, reinicie o Oracle VM Server.

   As tarefas do d2drestorevm e d2dverify são executadas com êxito.

A máquina virtual ESXi falha ao iniciar após a BMR a partir de uma máquina física

Sintoma

Eu executei uma BMR usando os pontos de recuperação de uma máquina física para uma máquina virtual ESXi. A máquina física usa um BIOS mais antigo. A BMR é concluída com êxito, mas o ESXi VM não é iniciado com êxito.

Solução

Modifique o tipo de controlador SCSI do ESXi VM de destino e envie a tarefa de BMR novamente.

Siga estas etapas:

1. Efetue logon no ESX Server.
2. Clique com o botão direito no ESXi VM de destino e selecione Editar configurações.
3. Na guia Hardware, selecione o controlador SCSI 0, e clique no botão de tipo de mudança.

   A caixa de diálogo Alterar tipo de controlador SCSI é exibida.
4. Selecione LSI Logic SAS e salve as configurações.
5. Envie uma tarefa de recuperação bare metal para essa VM.

   A máquina virtual é iniciada com êxito após a tarefa BMR.

Falha ao montar o CIFS no servidor ou nó de destino

Sintoma

Quando tento fazer backup ou restaurar usando CIFS, o CIFS falha ao montar no servidor ou no nó de destino.

Solução

Alguns requisitos devem ser satisfeitos durante a montagem do CIFS em um computador Linux.

Siga estas etapas:

1. Use o comando mount no servidor ou nó de destino para verificar o erro.
2. Quando usar um caminho compartilhado exportado de sistemas diferentes do Windows, verifique se a diferenciação de maiúsculas de minúsculas dos caracteres do caminho compartilhado corresponde o caminho original.
3. Se o comando mount retornar um erro, verifique se a hora no servidor ou nó de destino está sincronizada com a do servidor CIFS.
4. Se não encontrar o erro, adicione algumas opções para o comando mount para tentar novamente.

   Por exemplo, adicione "sec=ntlm" quando você receber o erro de permissão negada.

5. Ao diagnosticar o erro, siga estas etapas:

   Para falha de montagem do CIFS no servidor

   1. Abra o arquivo server.env em:

      /opt/Arcserve/d2dserver/configfiles/server.env

   2. Adicione todas as opções para o arquivo usando o seguinte comando:

      export D2D_MOUNTOPTION=<options>

   c. Salve o arquivo e reinicie o serviço.

   Para falha de montagem do CIFS no nó de destino

   1. Abra o arquivo .bashrc no caminho base do usuário.

      Exemplo: o local de um usuário é */home/user/* e da raiz é */root/*.

   2. Adicione todas as opções para o arquivo usando o seguinte comando:

      export D2D_MOUNTOPTION=<options>

   c. Salve o arquivo.

Observação: .bashrc é o arquivo recomendado aqui, mas você também poderia modificar outros arquivos como /ect/profile e /etc/bashrc, entre outros.

6. Quando usar um caminho compartilhado exportado de sistemas diferentes do Windows, verifique se a diferenciação de maiúsculas de minúsculas dos caracteres do caminho compartilhado corresponde o caminho original.

Falha na restauração no nível do arquivo em uma VM do Linux com base em host devido a um sistema de arquivos não suportado

Sintoma

Quando executo uma restauração no nível de arquivo para uma VM do Linux com base em host, o assistente de restauração exibe a seguinte mensagem de erro:

Não suportado: sistema de arquivos reiserfs

O erro ocorre porque você está tentando restaurar um sistema de arquivos não suportado.

Solução

Há duas maneiras de restaurar a VM do Linux com base em host:

- Use o Live CD do Agente do Arcserve UDP (Linux) para executar a restauração em nível de arquivo, já que o Live CD oferece suporte a todos os tipos de sistema de arquivos. Essa é uma solução conveniente, mas temporária. Você pode restaurar usando um Live CD se esse nó não tiver sido restaurado com frequência.
- Outro método permanente é que você pode instalar o driver do sistema de arquivos correto para oferecer suporte ao reiserfs ou ativar o driver correspondente que já está instalado no servidor de backup.

Não é possível restaurar o volume do sistema do SUSE15 com o sistema de arquivos XFS

Sintoma

Ao executar uma tarefa de restauração usando o ponto de recuperação do SUSE15 com o sistema de arquivos XFS, a tarefa de restauração falha, já que o volume do sistema não está montado. A seguinte mensagem de aviso é exibida no log de atividades: *Falha ao montar volume do sistema. O sistema pode não ser inicializado após a restauração.*

Solução

Crie um Live CD do CentOS 7.5 e use-o para executar BMR/instant BMR.sudo apt install apt-file.

Falha ao acessar o URL de Montar ponto de recuperação compartilhado pelo WebDAV

Sintoma

Ao executar a opção Montar ponto de recuperação que é compartilhada pelo WebDAV e acessada por vários usuários que utilizam o mesmo servidor de backup Linux, o acesso apenas ao primeiro URL é bem-sucedido, mas os URLs restantes falham.
Esse erro ocorre porque o Arcserve não oferece suporte ao acesso a URLs compartilhados por vários usuários a partir do mesmo navegador.

Solução

Use navegadores diferentes para acessar as URLs ou limpe os cookies e tente novamente.

A implantação de drivers Ubuntu usando o comando d2dupgradetool falha no Ubuntu20.04 LBS

Sintoma

Ao fazer download do arquivo de drivers e dos arquivos de assinatura, o comando curl gera o seguinte erro:

Erro de cURL 35: error:1414D172:SSL routines:tls12_check_peer_sigalg:wrong signature type

Solução

Atualize o OpenSSL 1.1.1f para o OpenSSL 1.1.1g no Ubuntu20.04 LBS.