

IBM Spectrum Protect for Virtual Environments  
Versão 8.1.0

*Proteção de Dados para VMware*





IBM Spectrum Protect for Virtual Environments  
Versão 8.1.0

*Proteção de Dados para VMware*



**Nota:**

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Aviso” na página 117.

Esta edição se aplica à versão 8, liberação 1, modificação 0 do IBM Spectrum Protect for Virtual Environments (número do produto 5725-X00) e a todas as liberações e modificações subsequentes até que seja indicado em contrário em novas edições.

© Copyright IBM Corporation 2011, 2016.

# Índice

<b>Sobre esta Publicação</b> . . . . .	<b>v</b>
Quem Deve Ler Esta Publicação . . . . .	v
Publicações . . . . .	v

<b>O Que Há de Novo na Versão 8.1</b> . . . .	<b>vii</b>
---	------------

## Capítulo 1. Instalando e Atualizando Proteção de Dados para VMware . . . . 1

Componentes Instaláveis . . . . .	1
GUI do Data Protection for VMware vSphere . . . . .	3
Agente de recuperação do IBM Spectrum Protect . . . . .	6
Extensão do IBM Spectrum Protect . . . . .	7
Interface da linha de comandos do Data Protection for VMware . . . . .	7
Interface da restauração do arquivo do IBM Spectrum Protect . . . . .	8
Recurso de movedor de dados . . . . .	8
Planejando instalar o Proteção de Dados para VMware . . . . .	9
Roteiro de Instalação . . . . .	9
Cenários de instalação . . . . .	10
Requisitos do Sistema . . . . .	11
Instalando os componentes do Proteção de Dados para VMware . . . . .	19
Obtendo o pacote de instalação do Proteção de Dados para VMware . . . . .	19
Instalando os componentes Proteção de Dados para VMware usando o assistente de instalação . . . . .	20
Instalando os componentes do Proteção de Dados para VMware no modo silencioso . . . . .	24
Executando as primeiras etapas após instalar o Proteção de Dados para VMware . . . . .	30
Fazendo Upgrade do Proteção de Dados para VMware . . . . .	32
Fazendo upgrade do Proteção de Dados para VMware . . . . .	32
Atualizando o Proteção de Dados para VMware em um Sistema Windows de 64 bits no Modo Silencioso . . . . .	33
Atualizando o Proteção de Dados para VMware em um Sistema Linux no Modo Silencioso . . . . .	34
Desinstalando o Proteção de Dados para VMware . . . . .	35
Desinstalando o Proteção de Dados para VMware nos sistemas Windows . . . . .	35
Desinstalando o Proteção de Dados para VMware for Windows em modo silencioso . . . . .	37
Desinstalando o Proteção de Dados para VMware em um sistema Linux . . . . .	38

## Capítulo 2. Configurando o Proteção de Dados para VMware . . . . . 41

Configurando uma nova instalação com o assistente . . . . .	41
Usando o bloco de notas para editar uma instalação existente . . . . .	42

Ativando o ambiente para operações de restauração de arquivo . . . . .	43
Configurando operações de restauração de arquivos no Linux . . . . .	44
Modificando opções para as operações de restauração de arquivo . . . . .	45
Opções de restauração de arquivo . . . . .	46
Configurando a atividade de log para operações de restauração de arquivo . . . . .	47
Opções de atividade do log de restauração de arquivos . . . . .	48
Configurando um nó do movedor de dados para suporte de identificação . . . . .	49
Configurando seu ambiente para operações de restauração instantânea de máquina virtual completa . . . . .	51
1. Configurando o software iSCSI no host ESXi . . . . .	52
2. Instalando e configurando aplicativos no movimentador de dados . . . . .	52
3. Configurando a conexão do Recovery Agent . . . . .	53
4. Configurando uma rede iSCSI dedicada para o host ESXi e o movimentador de dados . . . . .	53
Configurando a comunicação com Segurança da Camada de Transporte . . . . .	55
Usando um certificado de terceiros . . . . .	55
Ativando a comunicação segura com o servidor IBM Spectrum Protect . . . . .	60
Requisitos de privilégio de usuário do VMware vCenter Server . . . . .	61
Funções de Usuário do GUI do Data Protection for VMware vSphere . . . . .	64
Chaves de registro da GUI do Proteção de Dados para VMware . . . . .	67
Configurando a GUI do agente de recuperação . . . . .	68
Ativando a comunicação segura do agente de recuperação para o servidor IBM Spectrum Protect . . . . .	73
Configurações do código de idioma . . . . .	77
Atividade do arquivo de log . . . . .	77
Iniciando e Executando Serviços para Proteção de Dados para VMware . . . . .	80

## Apêndice A. Tarefas avançadas de configuração . . . . . 81

Configurando os Nós do IBM Spectrum Protect em um Ambiente vSphere . . . . .	82
Configurando Nós do Movedor de Dados em um Ambiente vSphere . . . . .	83
Configurando o Interface da linha de comandos do Data Protection for VMware em um ambiente do vSphere . . . . .	88
Lista de Verificação de Configuração da Interface da Linha de Comandos do Ambiente vSphere . . . . .	91
Diretrizes de Configuração de Fita . . . . .	94

Configurando manualmente um dispositivo iSCSI em um sistema Linux . . . . .	96
Configurando manualmente um dispositivo iSCSI em um sistema Windows . . . . .	99
Configurando manualmente o nós do proxy de montagem em um sistema Linux . . . . .	101
Configurando manualmente o nós do proxy de montagem em um sistema Windows remoto . . .	103
Configurando manualmente diversos serviços de client acceptor em um sistema Linux . . . . .	105
Modificando o Arquivo de Configuração VMCLI	107

<b>Apêndice B. Migrando para uma estratégia de backup incremental contínuo . . . . .</b>	<b>109</b>
--	------------

<b>Apêndice C. Recursos de Acessibilidade para a Família de Produtos IBM Spectrum Protect . . .</b>	<b>115</b>
---	------------

<b>Aviso . . . . .</b>	<b>117</b>
------------------------	------------

<b>Glossário . . . . .</b>	<b>121</b>
----------------------------	------------

<b>Índice Remissivo . . . . .</b>	<b>123</b>
-----------------------------------	------------

---

## Sobre esta Publicação

O IBM Spectrum Protect for Virtual Environments fornece backup incremental de nível de bloco fora do host, recuperação de arquivo e restauração instantânea a partir de um backup completo da MV para máquinas guest Windows e Linux. Os backups incrementais em nível de bloco estão disponíveis ao usar o IBM Spectrum Protect for Virtual Environments com o movedor de dados do IBM Spectrum Protect.

---

## Quem Deve Ler Esta Publicação

Esta publicação é destinada aos usuários e administradores que desejam instalar e configurar o IBM Spectrum Protect for Virtual Environments.

Informações gerais, tarefas do usuário, cenários de backup e restauração, referência de comando e mensagens de erro estão documentados no *IBM Spectrum Protect for Virtual Environments: Proteção de Dados para VMware User's Guide*.

---

## Publicações

A família de produtos IBM Spectrum Protect inclui IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for Databases e vários outros produtos de gerenciamento de armazenamento da IBM®.

Para visualizar a documentação do produto IBM, consulte IBM Knowledge Center.





---

## O Que Há de Novo na Versão 8.1

O Proteção de Dados para VMware Versão 8.1 introduz novos recursos e atualizações.

Para obter uma lista de novos recursos e atualizações nesta liberação, consulte Atualizações do Data Protection for VMware.



---

# Capítulo 1. Instalando e Atualizando Proteção de Dados para VMware

A instalação do Proteção de Dados para VMware inclui planejamento, instalação e configuração inicial.

---

## Componentes Instaláveis

O Proteção de Dados para VMware inclui vários componentes que podem ser instalados para proteger seu ambiente virtual.

Dependendo do ambiente do sistema operacional, os seguintes recursos do Proteção de Dados para VMware estão disponíveis para instalação:

**Restrição:** Cada pacote de instalação apresenta um arquivo de licenciamento de usuário (EULA). Se você não aceitar o arquivo, o processo de instalação será interrompido.

*Tabela 1. Recursos Disponíveis do Proteção de Dados para VMware por Sistema Operacional*

Componente	Linux	Windows
<b>Agente de recuperação do IBM Spectrum Protect</b> Este componente fornece recursos de montagem virtual e restauração instantânea.		√
<b>Interface da linha de comandos do agente de recuperação</b> A interface da linha de comandos usada para operações de montagem.		√
<b>Documentos Relacionados</b> Os documentos incluem os arquivos leia-me e de aviso.	√	√
<b>Arquivos de ativação do Data Protection for VMware</b> Este componente permite que o IBM Spectrum Protect execute os seguintes tipos de backup: <ul style="list-style-type: none"><li>• Backup incremental contínuo incremental</li><li>• Backup incremental contínuo completo</li></ul> Este componente é necessário para proteção de aplicativo. Se você transferir cargas de trabalho de backup, esse arquivo deverá ser instalado no Servidor de Backup vStorage.	√	√

*Tabela 1. Recursos Disponíveis do Proteção de Dados para VMware por Sistema Operacional (continuação)*

Componente	Linux	Windows
<b>GUI do Data Protection for VMware vSphere</b>  Esse componente é uma interface gráfica com o usuário (GUI) que acessa dados da MV no VMware vCenter Server. O conteúdo da GUI fica disponível em três visualizações: <ul style="list-style-type: none"> <li>• Uma visualização de navegador da web. Essa visualização é acessada em um navegador da web suportado, utilizando a URL do host do servidor da web da GUI. Por exemplo:  <a href="https://guihost.mycompany.com:9081/TsmVMwareUI/">https://guihost.mycompany.com:9081/TsmVMwareUI/</a></li> <li>• A visualização do Extensão do IBM Spectrum Protect no VMware vSphere Web Client. Esses painéis nessa visualização são projetados exclusivamente para integração dentro do Web Client, mas dados e comandos para essa visualização são obtidos do mesmo servidor da web da GUI que de outras visualizações. O Extensão do IBM Spectrum Protect fornece um subconjunto das funções que estão disponíveis na visualização do navegador da web e algumas funções adicionais. Funções de configuração e relatório avançado não são oferecidas nessa visualização.</li> </ul> É possível especificar uma ou mais visualizações durante a instalação.	√	√
<b>GUI de restauração de arquivo</b>  Esse componente é uma GUI baseada na web que permite restaurar arquivos de um backup de máquina virtual VMware sem assistência de administrador. A GUI será instalada automaticamente quando a GUI do Proteção de Dados para VMware for instalada. Ela é ativada por meio do assistente de configuração.	1	√
<b>Movedor de Dados</b>  O movedor de dados do IBM Spectrum Protect move dados para o Proteção de Dados para VMware. Essa funcionalidade é referida como o movedor de dados. O movedor de dados move dados do ambiente virtual para o servidor IBM Spectrum Protect. Ao instalar o movedor de dados em um servidor, o servidor poderá ser usado como um servidor de backup vStorage. É possível instalar o movedor de dados no mesmo sistema que o Proteção de Dados para VMware ou em outro servidor.	√	√

1. Embora o componente da interface de restauração do arquivo deva ser instalado e ativado em um sistema Windows, é possível usar essa interface para restaurar arquivos em máquinas virtuais guests Windows e Linux.

O Proteção de Dados para VMware transfere a carga de trabalho do backup das VMs para o servidor de backup vStorage. Para realizar essa tarefa, o movedor de dados V8.1.0 deve estar instalado no Servidor de Backup vStorage.

## GUI do Data Protection for VMware vSphere

O componente do GUI do Data Protection for VMware vSphere (GUI do vSphere) é uma interface gráfica com o usuário que acessa dados da VM no VMware vCenter Server.

### Visão Geral

O GUI do Data Protection for VMware vSphere é a interface primária da qual concluir as etapas a seguir:

- Inicie ou planeje os backups de suas VMs (máquinas virtuais) em um servidor IBM Spectrum Protect.
- Inicie uma recuperação completa de suas VMs (máquinas virtuais) a partir de um servidor IBM Spectrum Protect.
- Emita relatórios sobre o progresso de suas tarefas, os eventos mais recentes que foram concluídos, status de backup e uso de espaço. Essas informações podem ajudar a solucionar os problemas que ocorreram durante o processo de backup.

**Dica:** As informações sobre como concluir tarefas com a GUI do vSphere são fornecidas na ajuda on-line que é instalada com a GUI. Clique em **Saiba Mais** em qualquer uma das janelas da GUI para abrir a ajuda online e obter assistência de tarefa.

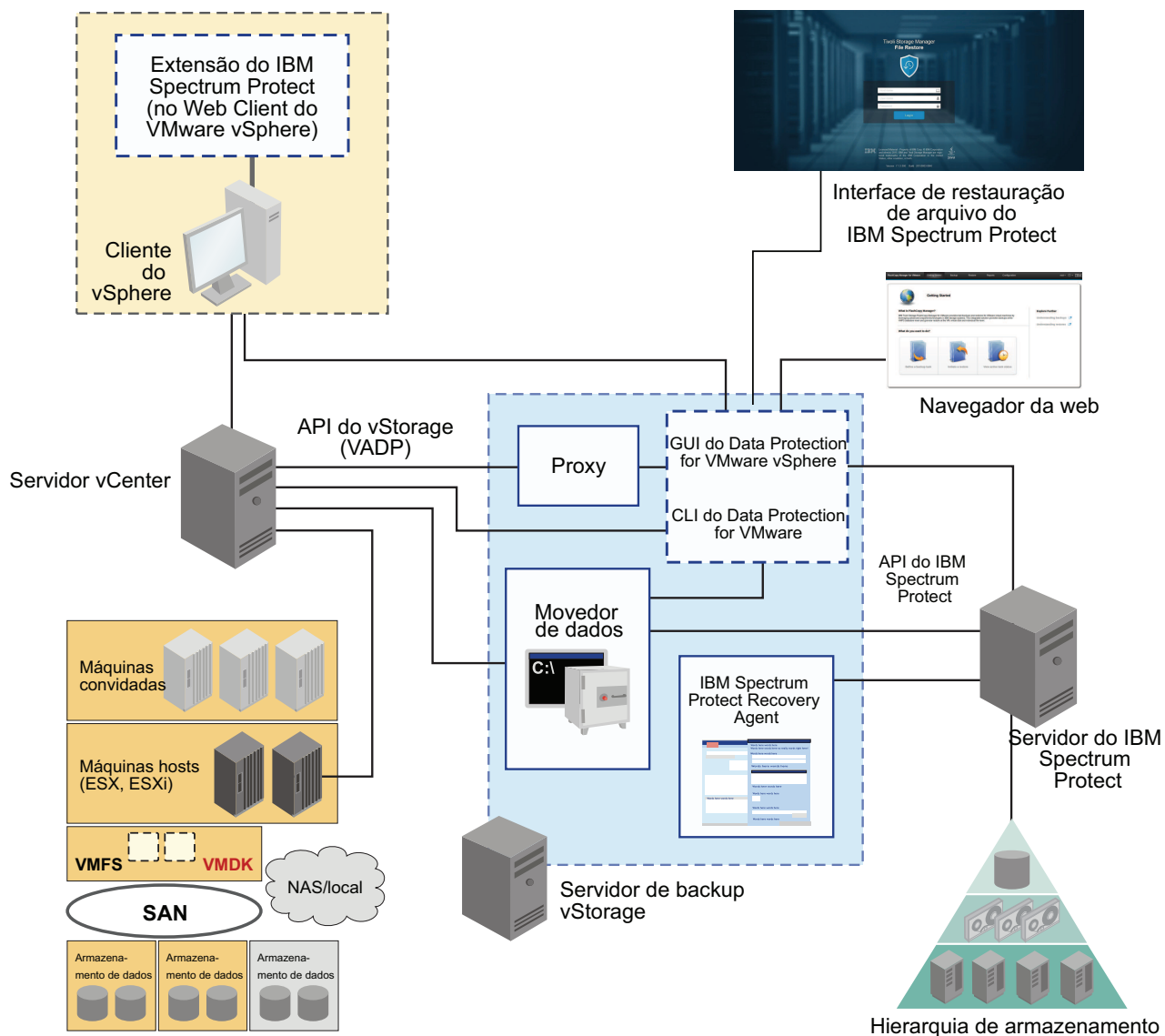


Figura 1. Componentes do Sistema Proteção de Dados para VMware em um Ambiente do Usuário do VMware vSphere

## Requisitos

O GUI do Data Protection for VMware vSphere pode ser instalado em qualquer sistema que atenda aos pré-requisitos do sistema operacional. Os requisitos de recurso da GUI do vSphere são mínimos, visto que ele não processa transferências de dados de E/S.

**Dica:** Instalar a GUI do vSphere no servidor de backup do vStorage é a configuração mais comum.

A GUI do vSphere deve ter a conectividade de rede para os sistemas a seguir:

- Servidor de Backup vStorage
- Servidor IBM Spectrum Protect
- vCenter Server

Além disso, as portas para o banco de dados Derby (padrão 1527) e o servidor da web da GUI (padrão 9081) devem estar disponíveis.

## Configuração

É possível registrar diversas GUIs do vSphere em um único servidor vCenter. Esse cenário reduz o número de datacenters (e seus backups convidados da VM) que são gerenciados por uma única GUI do VMware vSphere. Um vCenter Server poderá então gerenciar um subconjunto do número total de datacenters definidos no vCenter Server.

Para atualizar os datacenters gerenciados, acesse **Configuração > Configuração de edição**.

Ao registrar diversas GUIs do vSphere em um único servidor vCenter, as diretrizes a seguir serão aplicadas:

- Cada datacenter pode ser gerenciado por uma única GUI instalada do vSphere.
- Um nome do nó VMCLI exclusivo é necessário para cada GUI instalada do vSphere.
- Usar nomes do nó do movedor de dados exclusivos para cada GUI instalada do vSphere simplifica o gerenciamento dos nós.

## Acessando a GUI do vSphere

A GUI do vSphere é acessada pelos métodos a seguir:

- Uma GUI de navegador da web independente. Essa GUI é acessada por meio de um marcador de URL para o servidor da web da GUI, por exemplo:

`https://hostname:port/TsmVMwareUI/`

em que:

- *hostname* é o nome do sistema em que o GUI do Data Protection for VMware vSphere está instalado
- *port* é o número da porta através da qual a GUI do vSphere é acessível. O número da porta padrão é 9081.
- Uma extensão do vSphere Web Client que se conecta com um servidor da web da GUI para acessar máquinas virtuais no armazenamento da IBM (referido como uma extensão da proteção de dados). O conteúdo é um subconjunto do que é fornecido na GUI (interface gráfica com o usuário) do navegador da web.

É possível especificar um ou mais métodos de acesso durante a instalação.

### Windows

O diretório de instalação é `C:\IBM\tivoli\tsm\tdpvmware\webserver`.

### Linux

O diretório de instalação padrão é `/opt/tivoli/tsm/tdpvmware/common/webserver`.

## Agente de recuperação do IBM Spectrum Protect

Use o serviço do agente de recuperação para montar qualquer volume de captura instantânea do servidor IBM Spectrum Protect.

### Visão Geral

É possível visualizar as capturas instantâneas localmente, com acesso somente leitura, no sistema do cliente ou usar o protocolo iSCSI para acessar uma captura instantânea de um sistema remoto.

Além disso, o agente de recuperação fornece a função de restauração instantânea e a proteção de aplicativos convidados. A restauração instantânea permite que o volume usado continue disponível enquanto a operação de restauração continua em plano de fundo. A proteção de aplicativo ativa os aplicativos que estão instalados em uma máquina virtual guest, como o Microsoft Exchange Server e Microsoft SQL Server, para estar disponível para backup e proteção de restauração.

**Importante:** Durante a instalação do agente de recuperação para uma função de restauração instantânea, também deve-se selecionar o driver de dispositivo para instalação. Ele não é selecionado por padrão.

O driver de dispositivo não é necessário para proteção de aplicativo.

O agente de recuperação pode concluir as tarefas a seguir a partir de um sistema remoto:

- Reunir informações sobre os dados que podem ser restaurados, por exemplo:
  - Backup feito das VMs.
  - Capturas instantâneas para uma máquina virtual com backup concluído
  - Partições disponíveis em uma captura instantânea específica.
- Monte uma captura instantânea como um dispositivo virtual.
- Fornecer uma lista de dispositivos virtuais.
- Remova um dispositivo virtual.

Para obter informações detalhadas sobre comandos, parâmetros e códigos de retorno, consulte a seção de referência de comandos no *IBM Spectrum Protect for Virtual Environments: guia do usuário do Proteção de Dados para VMware*.

### Requisitos

**Windows** Em sistemas Windows, é possível instalar a GUI do agente de recuperação, a interface da linha de comandos e o driver de dispositivo.

### Acessando o agente de recuperação

**Windows** É possível acessar o agente de recuperação a partir do menu **Iniciar**: **Iniciar > IBM Spectrum Protect > IBM Spectrum Protect for Virtual Environments > IBM Spectrum Protect agente de recuperação**

**Windows** Alternativamente, é possível acessar a GUI e a interface da linha de comandos a partir de um prompt de comandos:

```
install_dir\TSM\recoveryagent\mount\RecoveryAgent.exe -notservice  
install_dir\TSM\recoveryagent\shell\RecoveryAgentShell.exe
```



em que *install\_dir* é o diretório de instalação. O padrão é C:\Program Files\Tivoli. Nos sistemas Windows, use Program Files (x86).

## Extensão do IBM Spectrum Protect

O Extensão do IBM Spectrum Protect é uma extensão de Web client do VMware que fornece uma visualização do GUI do Data Protection for VMware vSphere.

### Visão geral

O Extensão do IBM Spectrum Protect fornece um subconjunto das funções que estão disponíveis na visualização do navegador para o GUI do Data Protection for VMware vSphere e algumas funções adicionais.

### Exigência

Para instalar o Extensão do IBM Spectrum Protect, deve-se selecionar as opções a seguir ao executar o assistente de instalação do IBM Spectrum Protect for Virtual Environments.

- Na página Proteção do ambiente do assistente de instalação, clique em **Proteção do vSphere**.
- Na página Informações da GUI para proteção do vSphere, selecione **Ativar acesso à GUI por meio de um navegador da web** e **Registrar como uma extensão do Web client do vSphere**.

### Acessando a extensão da proteção de dados

É possível acessar a extensão do vSphere Web Client.

## Interface da linha de comandos do Data Protection for VMware

O Data Protection for VMware CLI é uma interface da linha de comandos com função completa que é instalada com o GUI do Data Protection for VMware vSphere.

### Visão Geral

É possível usar o Data Protection for VMware CLI para concluir as tarefas a seguir:

- Inicie ou planeje os backups de suas VMs (máquinas virtuais) em um servidor IBM Spectrum Protect.
- Inicie uma recuperação completa de suas VMs (máquinas virtuais), arquivos da VM ou discos da VM (VMDKs) a partir de um servidor IBM Spectrum Protect.
- Visualizar as informações de configuração sobre o banco de dados e o ambiente de backup.

Embora o GUI do Data Protection for VMware vSphere seja a interface de tarefa primária, o Data Protection for VMware CLI fornece uma interface secundária útil.

Por exemplo, o Data Protection for VMware CLI pode ser usado para implementar um mecanismo de planejamento que seja diferente de um que é implementado pelo GUI do Data Protection for VMware vSphere. Além disso, o Data Protection for VMware CLI será útil ao avaliar os resultados de automação com os scripts.

## **Acessando o Interface da linha de comandos do Data Protection for VMware**

É possível acessar o Data Protection for VMware CLI a partir de uma linha de comandos.

Para obter informações detalhadas sobre os comandos disponíveis, consulte a seção de referência de comando no *IBM Spectrum Protect for Virtual Environments: guia do usuário do Proteção de Dados para VMware*

## **Interface da restauração do arquivo do IBM Spectrum Protect**

É possível restaurar arquivos individuais a partir de um backup da máquina virtual VMware.

### **Visão Geral**

A interface de restauração do arquivo é uma interface baseada na web na qual é possível restaurar arquivos individuais a partir de um backup da VM. A vantagem dessa interface é que os proprietários do arquivo, do software e da plataforma podem restaurar seus próprios arquivos sem conhecimento anterior de operações de restauração e de backup do IBM Spectrum Protect.

O recurso de interface de restauração do arquivo está instalado quando você seleciona a opção de proteger seus dados em um ambiente vSphere. No assistente de configuração do Proteção de Dados para VMware, deve-se ativar o recurso de restauração do arquivo para a interface para ficar disponível.

### **Acessando a interface de restauração do arquivo do IBM Spectrum Protect**

Para acessar a interface de restauração do arquivo, abra um navegador da web e insira a URL fornecida pelo administrador. Por exemplo:

`https://hostname:9081/FileRestoreUI`

onde *hostname* é o nome do host do sistema onde o GUI do Data Protection for VMware vSphere está instalado.

## **Recurso de movedor de dados**

O movedor de dados é um nó cliente específico que "move" dados de um sistema para outro.

### **Visão Geral**

No ambiente do VMware típico, o nó do movedor de dados é usado para salvar backups de máquina virtual em um nó do datacenter.

Para obter mais informações sobre o movedor de dados, incluindo informações sobre ambientes com vários movedores de dados, consulte Como nós do IBM Spectrum Protect são usados em um ambiente virtual.

### **Acessando os arquivos de configuração do movedor de dados**

É possível configurar o movedor de dados da GUI do Proteção de Dados para VMware vSphere.

**Windows** O diretório de instalação padrão é C:\Program Files\Tivoli\TSM\baclient.

**Linux** O diretório de instalação padrão é /opt/tivoli/tsm/client/ba/bin.

## Planejando instalar o Proteção de Dados para VMware

O Proteção de Dados para VMware elimina o impacto da execução de backups em uma máquina virtual transferindo cargas de trabalho de backup de um baseado em ESXi ou ESX VMware para um servidor de Backup vStorage.

O Proteção de Dados para VMware trabalha com o movedor de dados (instalado no servidor de backup vStorage) para concluir backup completo incremental contínuo e backup incremental contínuo. O nó cliente que está instalado no servidor de backup vStorage é denominado o nó do movedor de dados. Esse nó "move" os dados para o servidor IBM Spectrum Protect para armazenamento e para a restauração em nível de imagem da MV posteriormente. A restauração instantânea está disponível em nível de volume do disco e nível de VM integral.

**Dica:** O movedor de dados é um componente licenciado separadamente que contém suas próprias interfaces com o usuário e documentação. A familiaridade com este produto e sua documentação é necessária para integrar adequadamente um plano abrangente de proteção a suas MVs com o Proteção de Dados para VMware. O Proteção de Dados para VMware for Windows de 64 bits inclui o recurso de movedor de dados.

## Roteiro de Instalação

A tabela a seguir identifica as etapas para concluir um processo de instalação com êxito.

*Tabela 2. Tarefas de instalação para clientes novos ou existentes do Proteção de Dados para VMware*

Etapa	Tarefa	Inicie aqui
1	Verificar os requisitos do sistema.	Certifique-se de que o sistema no qual o Proteção de Dados para VMware deve ser instalado atende os requisitos do sistema.
2	Verificar os requisitos de permissão de usuário.	Evite atrasos ou erros de instalação potenciais usando os níveis de permissão de usuário necessários.
3	Verificar a disponibilidade de portas de comunicação necessárias.	Evite atrasos ou falha na instalação abrindo as portas de comunicação necessárias antes de tentar instalar o Proteção de Dados para VMware.

*Tabela 2. Tarefas de instalação para clientes novos ou existentes do Proteção de Dados para VMware (continuação)*

Etapa	Tarefa	Inicie aqui
4	<p>Instalar o Proteção de Dados para VMware:</p> <ul style="list-style-type: none"> <li>• Instalando o Proteção de Dados para VMware usando o assistente de instalação</li> <li>• “Instalando os componentes do Proteção de Dados para VMware no modo silencioso” na página 24</li> </ul> <p>Fazer upgrade do Proteção de Dados para VMware:</p> <p>Fazer upgrade do Data Protection for VMware</p>	<p>Cada pacote de instalação apresenta um arquivo de licenciamento de usuário (EULA). Se você não aceitar o arquivo, a instalação será finalizada.</p>
5	<p>“Configurando uma nova instalação com o assistente” na página 41</p> <p>Se você estiver planejando fazer upgrade do Proteção de Dados para VMware, dependendo dos componentes que estão instalados, mais tarefas de configuração poderão ser necessárias. Consulte os tópicos de configuração no <i>IBM Spectrum Protect for Virtual Environments: guia do usuário do Proteção de Dados para VMware</i> para obter mais detalhes.</p>	<p>Use o assistente de configuração para uma configuração inicial. Dependendo dos recursos que estiverem instalados, mais tarefas de configuração poderão ser necessárias conforme descrito nesta seção.</p>

**Dica:** Para ajudar com o planejamento da quantidade de hosts do proxy que são necessários para seu ambiente de backup do Proteção de Dados para VMware específico, a publicação a seguir está disponível no wiki do IBM Spectrum Protect: [Step by Step Guide To vStorage Backup Server \(Proxy\) Sizing](#). Esta publicação está disponível na seção do produto IBM Spectrum Protect for Virtual Environments.

## Cenários de instalação

Antes de instalar o Proteção de Dados para VMware, escolha o cenário que melhor atende às necessidades de seus negócios.

É possível instalar o Proteção de Dados para VMware e o movedor de dados usando a GUI ou o modo silencioso:

- “Instalando os componentes Proteção de Dados para VMware usando o assistente de instalação” na página 20
- “Instalando os componentes do Proteção de Dados para VMware no modo silencioso” na página 24

Para obter uma lista de recursos e componentes que são disponíveis por plataforma, consulte “Componentes Instaláveis” na página 1.

Tabela 3. Cenários de instalação

Número de cenário	descrição	Tarefas que devem ser concluídas
1	Use este cenário para uma nova instalação em que deseje instalar o Proteção de Dados para VMware e o movedor de dados no mesmo sistema.	<p><b>Windows</b> É possível usar o Instalador do Conjunto na GUI ou no modo silencioso.</p> <p><b>Linux</b> É possível usar o InstallAnywhere na GUI ou no modo silencioso.</p>
2	Use este cenário para uma nova instalação na qual deseja instalar somente o Proteção de Dados para VMware.	<p><b>Windows</b> É possível concluir uma instalação customizada usando o Instalador do Conjunto para instalar o Proteção de Dados para VMware na GUI ou no modo silencioso.</p> <p><b>Linux</b> É possível concluir uma instalação customizada usando o InstallAnywhere para instalar o Proteção de Dados para VMware na GUI ou no modo silencioso.</p>
3	Use este cenário quando desejar instalar somente o movedor de dados em um sistema.	<p><b>Windows</b> É possível concluir uma instalação customizada usando o Instalador do Conjunto.</p> <p><b>Linux</b> O recurso de movedor de dados agora é instalado com o Proteção de Dados para VMware.</p>

## Requisitos do Sistema

Para implementar componentes do Proteção de Dados para VMware, seu sistema deve atender aos requisitos apropriados do sistema.

### Requisitos de software

Tabela 4. Requisitos de software para o Proteção de Dados para VMware.

Componente	Requisito Mínimo	Preferencial
Sistema Operacional	<b>Importante:</b> Os detalhes dos requisitos de software e sistema operacional podem ser alterados ao longo do tempo. Para obter os requisitos de software atuais, consulte nota técnica 1505139.	
Protocolo de comunicação		
Drivers de dispositivo		
Outro software		

### Requisitos de Hardware

Os requisitos de hardware variam dependendo dos seguintes itens:

- Número de servidores protegidos
- Número de volumes protegidos
- Tamanho dos conjuntos de dados

- Conectividade de LAN e SAN

**Nota:** O componente agente de recuperação não suporta operações em um ambiente sem a LAN.

A tabela a seguir descreve os requisitos de hardware necessários para instalar o Proteção de Dados para VMware.

*Tabela 5. Requisitos de Hardware para o Proteção de Dados para VMware*

Componente	Requisito Mínimo	Preferencial
Sistema	Processador IntelPentium D 3 GHz Dual Core ou compatível	Não aplicável
do NT	RAM de 2 GB, espaço de endereço virtual de 2 GB	Não aplicável
Disco rígido disponível	200 MB para a pasta 'Documents and Settings'	2 GB
Placa NIC	1 NIC - 100 Mbps	1 NIC - 1 Gbps

Um host do proxy do Windows é necessário para o agente de recuperação no Linux. Esse host do proxy do Windows deve ter o agente de recuperação instalado.

**Restrição:** As restrições a seguir são aplicadas aos VMware VMDKs que são envolvidos em uma operação de backup:

- Para modo de backup incremental contínuo, cada VMDK individual envolvido em uma operação de backup não pode exceder 8 TB. Se um VMDK exceder 8 TB, a operação de backup falhará. Para aumentar o tamanho do VMDK para torná-lo maior que o padrão de 2 TB, especifique o tamanho máximo com a opção `vmmaxvirtualdisks`. Para obter mais informações, consulte `Vmmaxvirtualdisks`.
- Para modo de backup completo incremental contínuo, cada VMDK individual envolvido em uma operação de backup não pode exceder 2 TB. Se um VMDK exceder 2 TB, a operação de backup falhará.

Para evitar uma falha durante o modo de backup, é possível ignorar o processamento do VMDK especificando `vmskipmaxvirtualdisks yes` no arquivo de opções do movedor de dados. Para obter mais informações, consulte `Vmskipmaxvirtualdisks`.

## Permissões de Instalação Necessárias

Antes de iniciar a instalação, certifique-se de que seu ID do usuário contenha o nível de permissão necessário.

## Sobre Esta Tarefa

*Tabela 6. Permissões de usuários necessárias para instalar e configurar o Proteção de Dados para VMware*

Sistema	Permissão necessária
Windows	Administrator
Linux	Root

Tabela 6. Permissões de usuários necessárias para instalar e configurar o Proteção de Dados para VMware (continuação)

Sistema	Permissão necessária
vCenter Server	<p>Privilegios de administrador</p> <p>A função do servidor vCenter requer os privilégios a seguir: <b>Extensão &gt; Registrar extensão, Cancelar registro de extensão, Atualizar extensão</b> Essa nova função deve ser aplicada ao objeto vCenter na hierarquia do servidor VMware vCenter para o ID do usuário que é especificado durante a instalação.</p>
<p>Servidor IBM Spectrum Protect</p> <p><b>Restrição:</b> O servidor deve ser iniciado.</p>	<p>Acesso administrativo</p> <p>(privilegio <b>Sistema</b> ou <b>Política de Domínio Irrestrita</b>)</p>

## Portas de Comunicação Necessárias

Visualize uma lista de portas de comunicação que devem ser abertas no firewall durante a instalação do Proteção de Dados para VMware.

As portas que são identificadas na tabela refletem uma instalação típica. Uma instalação típica consiste nos seguintes componentes no mesmo sistema Windows:

- Servidor Data Protection for VMware GUI
- Servidor de backup do vStorage (movedor de dados)
- Proxy de montagem Windows
- Interface da restauração do arquivo do IBM Spectrum Protect

Se uma instalação não típica for usada, mais portas poderão ser necessárias.

**Restrição:** O proxy de montagem Windows e o proxy de montagem Linux devem estar na mesma sub-rede.

Tabela 7. Portas de Comunicação Necessárias. Esta tabela identifica as portas que são acessados pelo Proteção de Dados para VMware.

Porta TCP	Iniciador: Saída (Do Host)	Destino: Entrada (Para o Host)
443	Servidor de Backup vStorage	vCenter Server (HTTP seguro)
443	Servidor GUI do Data Protection for VMware vSphere	vCenter Server
443  Essa configuração é necessária somente quando o movedor de dados é um sistema Linux.	Proxy de montagem Windows	vCenter Server
902  443	vCenter Server	hosts ESXi
902  443	vStorage Backup Server (proxy)	Hosts ESXi (todos os hosts protegidos)

*Tabela 7. Portas de Comunicação Necessárias (continuação).* Esta tabela identifica as portas que são acessados pelo Proteção de Dados para VMware.

Porta TCP	Iniciador: Saída (Do Host)	Destino: Entrada (Para o Host)
1500 ( <b>tcpport</b> )	vStorage Backup Server (proxy)	Servidor IBM Spectrum Protect
1500 ( <b>tcpadminport</b> )	<p>Servidor GUI do Data Protection for VMware vSphere</p> <ul style="list-style-type: none"> <li>1500 (<b>tcpadminport</b>) é comunicação não SSL</li> <li>Para a comunicação de SSL, <b>tcpadminport</b> é a única porta que suporta comunicação de SSL com o servidor IBM Spectrum Protect. O número da porta correto a ser usado para o protocolo SSL geralmente é o valor especificado pela opção <b>ssltcpadminport</b> no arquivo <code>dsmserv.opt</code> do servidor IBM Spectrum Protect. No entanto, se <b>adminonclient no</b> estiver especificado no arquivo <code>dsmserv.opt</code>, o número da porta correto a ser usado para o protocolo SSL será o valor especificado pela opção <b>ssltcpadminport</b>. A opção <b>ssltcpadminport</b> não tem um valor padrão. Portanto, o valor deve ser especificado pelo usuário.</li> </ul>	Servidor IBM Spectrum Protect
1527  Banco de dados Derby interno		
1501  1581 ( <b>httpport</b> )	Servidor IBM Spectrum Protect	<p>Servidor de Backup vStorage</p> <ul style="list-style-type: none"> <li>Planejador do movedor de dados</li> <li>Cliente Web</li> <li>Client Acceptor Daemon</li> </ul>
1581 ( <b>httpport</b> )  1582, 1583 ( <b>webports</b> )	Servidor GUI do Data Protection for VMware vSphere	Servidor de Backup vStorage
9081  Servidor da web da GUI (protocolo HTTPS)	vSphere Client	Servidor GUI do Data Protection for VMware vSphere (porta HTTPS segura para acesso ao vCenter por meio do navegador da web)
22  Porta padrão SSH para o agente de recuperação	Agente de recuperação	<p>Host de "montagem" do Proteção de Dados para VMware Windows</p> <ul style="list-style-type: none"> <li>SSH para o agente de recuperação Linux</li> </ul>



*Tabela 7. Portas de Comunicação Necessárias (continuação).* Esta tabela identifica as portas que são acessados pelo Proteção de Dados para VMware.

Porta TCP	Iniciador: Saída (Do Host)	Destino: Entrada (Para o Host)
3260	Restauração de arquivo do Linux Proteção de Dados para VMware	Host de "montagem" do Proteção de Dados para VMware Windows • iSCSI
3260 Porta padrão iSCSI para o agente de recuperação	Destino do Windows com o disco dinâmico para restauração de arquivo	Host de "montagem" do Proteção de Dados para VMware Windows • iSCSI
5985	Operações da GUI (interface gráfica com o usuário) de restauração de arquivos	Gerenciamento remoto do Windows
135	Proxy de montagem Windows	Máquina virtual VMware que contém os arquivos a serem restaurados com a interface de restauração de arquivos do IBM Spectrum Protect

## Requisitos de privilégio de usuário do VMware vCenter Server

Certos privilégios do VMware vCenter Server são necessários para executar operações do Proteção de Dados para VMware.

### Privilégios do vCenter Server necessários para proteger datacenters do VMware com a visualização do navegador da web para o GUI do Data Protection for VMware vSphere

O ID do usuário do vCenter Server que efetua sign on na visualização do navegador para o GUI do Data Protection for VMware vSphere

deve ter privilégios suficientes do VMware para visualizar o conteúdo de um datacenter gerenciado pela GUI.

Por exemplo, um ambiente VMware vSphere contém cinco datacenters. Um usuário, "jenn", tem privilégios suficientes para somente dois desses datacenters. Como resultado, somente esses dois datacenters, nos quais existem privilégios suficientes, são visíveis para "jenn" nas visualizações. Os outros três datacenters (para os quais "jenn" não tem privilégios) não estarão visíveis para o usuário "jenn".

O VMware vCenter Server define um conjunto de privilégios coletivamente como uma função. Uma função é aplicada a um objeto para um usuário ou grupo especificado para criar um privilégio. No VMware vSphere Web Client, você deve criar uma função com um conjunto de privilégios. Para criar uma função do vCenter Server para as operações de backup e restauração, use a função **Incluir uma Função** do VMware vSphere Client. Você deve designar esta função a um ID do usuário para um vCenter Server ou datacenter especificado. Se desejar propagar os privilégios para todos os datacenters dentro do vCenter, especifique o vCenter Server e marque a caixa de seleção propagar para filhos. Caso contrário, é possível limitar as permissões se designar a função para os datacenters necessários

apenas com a caixa de seleção propagar para os filhos selecionada. A execução da GUI do navegador é no nível do datacenter.

O seguinte exemplo mostra como controlar o acesso aos datacenters para dois grupos de usuário do VMware. Primeiro, crie uma função que contenha todos os privilégios definidos na nota técnica 7047438. O conjunto de privilégios neste exemplo é identificado pela função chamada “TDPVMwareManage”. O Grupo 1 requer acesso para gerenciar máquinas virtuais para os datacenters Primary1\_DC e Primary2\_DC. O Grupo 2 requer acesso para gerenciar máquinas virtuais para os datacenters Secondary1\_DC e Secondary2\_DC.

Para o Grupo 1, designe a função “TDPVMwareManage” para os datacenters Primary1\_DC e Primary2\_DC. Para o Grupo 2, designe a função “TDPVMwareManage” para os datacenters Secondary1\_DC e Secondary2\_DC.

Os usuários em cada grupo de usuários do VMware podem usar a GUI do Proteção de Dados para VMware para gerenciar máquinas virtuais apenas em seus respectivos datacenters.

**Dica:** Ao criar uma função, considere incluir privilégios extras na função que você pode precisar posteriormente para concluir outras tarefas em objetos.

### **Privilégios do vCenter Server necessários para usar o movedor de dados**

O movedor de dados do IBM Spectrum Protect instalado no servidor de backup vStorage (o nó do movedor de dados) requer as opções VMCUser e VMCPw. A opção VMCUser especifica o ID do usuário do servidor vCenter ou ESX que deseja fazer backup, restaurar ou consultar. Os privilégios necessários que são designados ao ID do usuário (VMCUser) asseguram que o cliente possa executar operações na máquina virtual e no ambiente VMware. Este ID do usuário deve ter os privilégios do VMware que são descritos em nota técnica 7047438.

Para criar uma função do vCenter Server para as operações de backup e restauração, use a função **Incluir uma Função** do VMware vSphere Client. Deve-se selecionar a opção propagar para os filhos ao incluir privilégios para esse ID do usuário (VMCUser). Além disso, considere incluir outros privilégios a essa função para tarefas diferentes de backup e restauração. Para a opção VMCUser, a execução está no objeto de nível superior.

### **Privilégios do vCenter Server necessários para proteger datacenters do VMware com a visualização do Extensão do IBM Spectrum Protect para o GUI do Data Protection for VMware vSphere**

O Extensão do IBM Spectrum Protect requer um conjunto de privilégios que são separados dos privilégios necessários para efetuar sign on na GUI.

Durante a instalação, os seguintes privilégios customizados são criados para o Extensão do IBM Spectrum Protect:

- **Datacenter > IBM Data Protection**
- **Global > IBM Data Protection**

Os privilégios customizados requeridos para o Extensão do IBM Spectrum Protect são registrados como uma extensão separada. A chave de extensão de privilégios é `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Esses privilégios permitem que o administrador do VMware ative e desative o acesso ao conteúdo do Extensão do IBM Spectrum Protect. Apenas os usuários com esses privilégios customizados no objeto do VMware requerido podem acessar o conteúdo do Extensão do IBM Spectrum Protect. Um Extensão do IBM Spectrum Protect é registrado para cada vCenter Server e é compartilhado por todos os hosts da GUI que são configurados para suportar o vCenter Server.

No Web client do VMware vSphere, deve-se criar uma função para os usuários que podem executar funções de proteção de dados para máquinas virtuais, utilizando o Extensão do IBM Spectrum Protect. Para essa função, além dos privilégios da função de administrador da máquina virtual padrão requeridos pelo web client, você deve especificar o privilégio **Datacenter > IBM Data Protection**. Para cada datacenter, designe esta função para cada usuário ou grupo de usuários em que deseja conceder permissão para o usuário gerenciar máquinas virtuais.

O privilégio **Global > IBM Data Protection** é necessário para o usuário no nível do vCenter. Esse privilégio permite que o usuário gerencie, edite ou limpe a conexão entre o vCenter Server e o servidor da web do GUI do Data Protection for VMware vSphere. Designe esse privilégio para os administradores que estão familiarizados com o GUI do Data Protection for VMware vSphere que protege seus respectivos vCenter Servers. Gerencie suas conexões do Extensão do IBM Spectrum Protect na página Conexões da extensão.

O seguinte exemplo mostra como controlar o acesso aos datacenters para dois grupos de usuário. O grupo 1 requer acesso para gerenciar máquinas virtuais para os datacenters NewYork\_DC e Boston\_DC. O grupo 2 requer acesso para gerenciar máquinas virtuais para os datacenters LosAngeles\_DC e SanFrancisco\_DC.

No cliente VMware vSphere, crie, por exemplo, a função “IBMDDataProtectManage”, designe os privilégios de função de administrador da máquina virtual padrão e também o privilégio do **Datacenter > IBM Data Protection**.

Para o Grupo 1, designe a função “IBMDDataProtectManage” para os datacenters NewYork\_DC e Boston\_DC. Para o Grupo 2, designe a função “IBMDDataProtectManage” para os datacenters LosAngeles\_DC e SanFrancisco\_DC.

Os usuários em cada grupo podem usar o Extensão do IBM Spectrum Protect no Web client do vSphere para gerenciar máquinas virtuais apenas em seus respectivos datacenters.

## **Problemas relacionados a permissões insuficientes**

Quando o usuário do navegador da web não tem permissões suficientes para nenhum datacenter, o acesso à visualização é bloqueado. Em vez disso, a mensagem de erro GVM2013E é emitida para avisar que o usuário não está autorizado a acessar nenhum datacenter gerenciado devido a permissões insuficientes. Estão disponíveis também outras mensagens novas que informam aos usuários sobre os problemas que resultam de permissões insuficientes. Para resolver quaisquer problemas relacionados a permissões, assegure-se de que a função de usuário esteja configurada conforme descrito nas seções anteriores. A função de usuário deve ter todos os privilégios identificados na tabela de IDs de usuários e movedores de dados de privilégios requeridos do vCenter Server e esses privilégios devem ser aplicados no nível do datacenter com a caixa de seleção propagar para filhos.

Quando o usuário do Extensão do IBM Spectrum Protect não tem permissões suficientes para um datacenter, as funções de proteção de dados para esse datacenter e seu conteúdo ficam indisponíveis na extensão.

Quando o ID do usuário IBM Spectrum Protect (especificado pela opção VMCUser) contém permissões insuficientes para as operações de backup ou restauração, a seguinte mensagem é exibida:

```
ANS9365E Erro de API do VMware vStorage.  
"A permissão para executar essa operação foi negada."
```

Quando o ID do usuário do IBM Spectrum Protect contém permissões insuficientes para visualizar uma máquina, as mensagens a seguir são mostradas:

```
Comando de backup da VM iniciado. Número total de máquinas virtuais a processar: 1  
ANS4155E A Máquina Virtual 'tango' não pôde ser localizada no servidor VMware.  
ANS4148E Um backup completo da Máquina Virtual 'foxtrot' falhou com o RC 4390
```

Para recuperar as informações de log por meio do VMware Virtual Center Server sobre problemas de permissão, conclua essas etapas:

1. Em Configurações do vCenter Server, selecione **Opções de criação de log** e configure **"Criação de log do vCenter** como **Trivial (Trivial)**.
2. Recrie o erro de permissão.
3. Reconfigure **Criação de log do vCenter** para seu valor anterior para evitar registrar informações de log em excesso.
4. Em Logs do sistema, procure o log mais atual do vCenter Server (vpxd-wxyz.log) e procure a sequência NoPermission. Por exemplo:  

```
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:  
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE  
Throw: vim.fault.NoPermission
```

Essa mensagem de log indica que o ID do usuário não continha permissões suficientes para criar uma captura instantânea (createSnapshot).

## Chaves de registro da GUI do Proteção de Dados para VMware

Dependendo das opções selecionadas durante a instalação, será possível acessar a GUI do Proteção de Dados para VMware usando métodos diferentes. Chaves de registro são criadas para as GUIs do Proteção de Dados para VMware.

A frase "GUI do Proteção de Dados para VMware" se aplica às GUIs a seguir:

- GUI do Data Protection for VMware vSphere acessada em um navegador da web
- Extensão do IBM Spectrum Protect na GUI do vSphere Web Client

A chave de registro do Extensão do IBM Spectrum Protect é `com.ibm.tsm.tdpvmware.IBMDDataProtection`. Essa chave é registrada ao selecionar a caixa de opções **Registrar a extensão do vSphere Web Client** durante a instalação. Uma única instância do Extensão do IBM Spectrum Protect é registrada por servidor vCenter.

Uma chave de registro não é criada para o GUI do Data Protection for VMware vSphere que é acessado em um navegador da web.

Para visualizar as chaves de registro, efetue login no VMware Managed Object Browser (MOB). Após efetuar login no MOB, acesse **Conteúdo>Gerenciador de Extensões** para visualizar as chaves de registro.



---

## Instalando os componentes do Proteção de Dados para VMware

É possível instalar todos ou alguns dos componentes que estão disponíveis no pacote do Proteção de Dados para VMware para seu sistema operacional.

### Sobre Esta Tarefa

Usando o instalador do Proteção de Dados para VMware, é possível instalar os componentes a seguir:

- Agente de recuperação do IBM Spectrum Protect
-  Interface da linha de comandos do agente de recuperação
-  Documentação (arquivo leia-me e arquivo de aviso)
- Proteção de Dados para VMwareArquivo de ativação
- GUI do Data Protection for VMware vSphere
- Recurso do movedor de dados, que inclui os seguintes itens:
  - GUI do movedor de dados
  - Web client do movedor de dados
  - Arquivos de tempo de execução da API do cliente (64 bits)
  - Linha de comandos do cliente administrador
  - Arquivos de tempo de execução da API do VMware vStorage

**Dica:** É possível criar diversos movedores de dados no mesmo sistema que o software Proteção de Dados para VMware ou é possível criar movedores de dados nos sistemas remotos. Essa configuração aumenta os recursos disponíveis para uso pelo Proteção de Dados para VMware. Os sistemas com o movedor de dados instalado são chamados servidores de backup do vStorage.

## Obtendo o pacote de instalação do Proteção de Dados para VMware

É possível obter o pacote de instalação do Proteção de Dados para VMware de um site de download da IBM, como o IBM Passport Advantage.

 Linux

### Antes de Iniciar

Se você planejar fazer download dos arquivos, configure o limite do usuário do sistema para o tamanho máximo do arquivo como ilimitado, para assegurar que os arquivos possam ser transferidos por download corretamente:

1. Para consultar o valor do tamanho máximo do arquivo, emita o comando a seguir:  
`ulimit -Hf`
2. Se o limite do usuário do sistema para o tamanho máximo do arquivo não estiver configurado como ilimitado, altere-o para ilimitado seguindo as instruções na documentação para seu sistema operacional.

### Procedimento

1. Faça download do arquivo de pacote apropriado a partir de um dos websites a seguir:

- Para uma instalação de primeira vez ou uma nova liberação, acesse Passport Advantage em: <http://www.ibm.com/software/lotus/passportadvantage/>. O Passport Advantage é o único site do qual é possível fazer download de um arquivo de pacote licenciado.
  - Para as informações, atualizações e correções de manutenção mais recentes acesse o site de suporte do IBM Spectrum Protect: [http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli\\_Storage\\_Manager](http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager).
2. Se você tiver transferido por download o pacote de um site de download da IBM, conclua as etapas a seguir:
    - a. Faça download do arquivo do pacote para o diretório de sua opção. O caminho deve conter no máximo 40 caracteres. Certifique-se de extrair os arquivos de instalação para um diretório vazio. Não extraia para um diretório que contenha arquivos extraídos anteriormente ou quaisquer outros arquivos.
    - b. **Linux** Certifique-se de que a permissão executável esteja configurada para o pacote. Se necessário, mude as permissões de arquivo, emitindo o comando a seguir:
 

```
chmod a+x package_name.bin
```
    - c. **Linux** Extraia o pacote emitindo o seguinte comando:
 

```
./package_name.bin
```

em que *package\_name* é o nome do arquivo transferido por download, por exemplo, 8.1.0.000-TIV-TSM4VE-LinuxX64.bin.
    - d. **Windows** Extraia o pacote clicando duas vezes em *package\_name*, em que *package\_name* é o nome do arquivo transferido por download; por exemplo, 8.1.0.000-TIV-TSM4VE-Windows.exe.

## Instalando os componentes Proteção de Dados para VMware usando o assistente de instalação

É possível instalar os componentes do Proteção de Dados para VMware usando o assistente de instalação.

### Sobre Esta Tarefa

**Windows** É possível usar o Suite Installer para instalar o Proteção de Dados para VMware e o movedor de dados.

**Linux** É possível utilizar o instalador independente para instalar o Proteção de Dados para VMware e o movedor de dados.

### Instalando os componentes do Proteção de Dados para VMware em sistemas Windows

Instalar os componentes e os recursos do Proteção de Dados para VMware usando o assistente de instalação.

### Antes de Iniciar

Antes de instalar os componentes do Proteção de Dados para VMware, assegure-se de atender os requisitos a seguir:

- Um ID de usuário com acesso de privilégio de administrador.
- A conectividade de rede com um VMware vCenter Server 5.x (ou mais recente) com acesso de privilégio de administrador.

- Conectividade de rede para um servidor IBM Spectrum Protect com acesso de administrador (privilegio **System** ou **Unrestricted Policy Domain**). Esse servidor deve estar disponível e em execução.
- Assegure-se de ter revisado os requisitos a seguir:
  - “Requisitos do Sistema” na página 11
  - “Permissões de Instalação Necessárias” na página 12
  - “Portas de Comunicação Necessárias” na página 13

Antes de instalar Proteção de Dados para VMware, você deve estar ciente das seguintes opções:

### **Tipo de Instalação**

#### **Instalação típica**

Com instalações típicas, todos os componentes e recursos do Proteção de Dados para VMware são instalados.

#### **Instalação Avançada**

Com instalações avançadas, é possível selecionar os componentes e recursos que deseja instalar.

### **Proteção de ambiente em um ambiente vSphere**

Com o GUI do Data Protection for VMware vSphere, é possível fazer backup, restaurar e gerenciar VMs em um ambiente do VMware vCenter.

### **Sobre Esta Tarefa**

É possível usar o Instalador do Conjunto para instalar o Proteção de Dados para VMware. O arquivo `spinstall.exe` para o Instalador do Conjunto está localizado na raiz do pacote de instalação.

Para obter uma lista de componentes e recursos que podem ser instalados, consulte “Componentes Instaláveis” na página 1.

### **Procedimento**

Para instalar o Proteção de Dados para VMware, conclua as etapas a seguir a partir do local do arquivo `spinstall.exe` para o componente escolhido para instalação:

1. Dê um clique duplo no arquivo `spinstall.exe`.
2. Siga as instruções do assistente para instalar os componentes selecionados. Ao instalar o agente de recuperação para uma restauração instantânea, você também deve selecionar o driver de dispositivo para instalação. Ele não é selecionado por padrão.

### **O que Fazer Depois**

Para acessar o GUI do Data Protection for VMware vSphere, consulte o seguinte:

- “Acessando o GUI do Data Protection for VMware vSphere” na página 31

O assistente de configuração será exibido automaticamente da primeira vez que a GUI for iniciada.

## Instalando o Proteção de Dados para VMware em sistemas Linux

Instale o Proteção de Dados para VMware em sistemas Linux usando o modo InstallAnywhere.

### Antes de Iniciar

Antes de instalar o Proteção de Dados para VMware, assegure-se de atender aos requisitos a seguir:

- Assegure-se de que o ID do usuário tenha o nível de permissão necessário e de que as portas de comunicação necessárias estejam abertas antes de continuar.
- O processo de instalação cria o usuário `tdpvmware`. Você deve emitir todos os comandos **vmcli** como o usuário `tdpvmware` e com o ID do usuário raiz.
- O X Window Server é necessário ao instalar no modo do console.
- Assegure-se de ter revisado os requisitos a seguir:
  - “Requisitos do Sistema” na página 11
  - “Permissões de Instalação Necessárias” na página 12
  - “Portas de Comunicação Necessárias” na página 13

### Procedimento

Para instalar a Proteção de Dados para VMware, execute as seguintes etapas:

1. A partir da raiz da pasta de instalação, mude os diretórios para `CD/Linux/DataProtectionForVMware`.
2. A partir de uma linha de comandos, insira o comando a seguir:  
`./install-Linux.bin`

### Resultados

Se você receber algum aviso ou erro, verifique os arquivos de log para obter informações adicionais. Consulte a “Atividade do arquivo de log” na página 77.

Se você não puder instalar o Proteção de Dados para VMware, por causa de uma falha, consulte o procedimento “Removendo manualmente o Proteção de Dados para VMware” em “Desinstalando o Proteção de Dados para VMware em um sistema Linux” na página 38.

### Executando uma instalação limpa do Proteção de Dados para VMware no Linux

Se uma instalação do Linux for interrompida, geralmente, será possível reiniciá-la. No entanto, se a instalação falhar ao ser reiniciada, uma instalação limpa será necessária.

### Sobre Esta Tarefa

Antes de iniciar uma instalação limpa, assegure-se de que o produto seja removido. Execute as seguintes etapas para garantir um ambiente limpo:

### Procedimento

1. Se o GUI do Data Protection for VMware vSphere estiver instalado, conclua estas tarefas:
  - a. Pare o Interface da linha de comandos do Data Protection for VMware emitindo este comando:  
`/etc/init.d/vmcli stop`



- b. Para o Servidor da Web da GUI do Proteção de Dados para VMware emitindo este comando:  
`/etc/init.d/webserver stop`
  - c. Remova o pacote .rpm emitindo este comando:  
`rpm -e TIVsm-TDPVMwarePlugin`
2. Remova as entradas do produto Deployment Engine:
  - a. Emita o comando a seguir para listar todas as entradas do Deployment Engine:  
`/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
  - b. Emita o comando a seguir para remover todas as entradas do Deployment Engine:  
`/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>`
  - c. Remova o diretório `/var/ibm/common`.
  - d. Remova o diretório `/usr/ibm/common`.
  - e. Limpe o diretório `/tmp` removendo o arquivo `acu_de.log`, se ele existir.
  - f. Remova o diretório `/tmp` que contém o ID do usuário que instalou o Deployment Engine.
  - g. Remova todas as entradas do Deployment Engine do arquivo de sistema `/etc/inittab`. As entradas são delimitadas por `#Begin AC Solution Install block` e `#End AC Solution Install block`. Remova todo o texto entre esses delimitadores e remova o próprio texto delimitador.
  - h. Remova todas as referências do Deployment Engine do arquivo de sistema `/etc/services`.
3. Remova todos os arquivos do Proteção de Dados para VMware da instalação com falha:
  - a. Remova os arquivos no `<USER_INSTALL_DIR>`, que é o caminho onde a instalação com falha foi tentada. Por exemplo, `/opt/tivoli/tsm/TDPVMware/`
  - b. Remova qualquer atalho da área de trabalho.
4. Faça backup do arquivo de registro global (`/var/.com.zerog.registry.xml`). Após o backup desse arquivo, remova todas as tags que referenciam o Proteção de Dados para VMware.
5. Remova os arquivos de log sob a raiz que contenham a sequência TDPVMware. Por exemplo:  
`IA-TDPVMware-00.log` ou `IA-TDPVMware_Uninstall-00.log`.
6. Remova o usuário que executou o Interface da linha de comandos do Data Protection for VMware.
  - a. Emita o seguinte comando:  
`userdel -r tdpvmware`
  - b. Emita o seguinte comando:  
`groupdel tdpvmware`

**Dica:** Em algumas versões do Linux, o comando **userdel** também remove o grupo quando não existe nenhum outro usuário associado. Como resultado, ignore qualquer mensagem de falha relacionada ao comando.

## Resultados

Uma vez concluídas essas etapas, inicie a instalação limpa.

## Instalando os componentes do Proteção de Dados para VMware no modo silencioso

É possível instalar o Proteção de Dados para VMware no segundo plano. Durante esta instalação silenciosa, nenhuma mensagem será exibida.

### Sobre Esta Tarefa

**Windows** É possível usar o Suite Installer para instalar o Proteção de Dados para VMware e o movedor de dados.

**Linux** É possível utilizar o instalador independente para instalar o Proteção de Dados para VMware e o movedor de dados.

### Instalar Proteção de Dados para VMware em sistemas Windows em modo silencioso

Instale todos os componentes do Proteção de Dados para VMware e o recurso do movedor de dados usando o Instalador do Conjunto em modo silencioso.

### Antes de Iniciar

Antes de instalar o recurso do Proteção de Dados para VMware e do movedor de dados, assegure-se de que seu sistema atenda aos requisitos nas seções a seguir:

- “Requisitos do Sistema” na página 11
- “Permissões de Instalação Necessárias” na página 12
- “Portas de Comunicação Necessárias” na página 13

Use os seguintes parâmetros do Proteção de Dados para VMware com os recursos de instalação silenciosa:

Tabela 8. Parâmetros de instalação silenciosa do Proteção de Dados para VMware

Parâmetro	descrição	Valor padrão
<b>ISFeatureInstall</b>	Especifique uma das opções a seguir ou ambas:  <b>TSM4VE</b> Instale todos os recursos do Data Protection for VMware, exceto o driver de dispositivo do agente de recuperação.  <b>Cliente</b> Instale todos os recursos do movedor de dados.	TSM4VE,Client
<b>ComponentsToInstallVe</b>	Especifique os recursos do Data Protection for VMware para instalar. Use os recursos descritos em Tabela 9 na página 26	Nenhuma
<b>ComponentsToInstallBa</b>	Especifique os recursos de movimentação de dados para instalar. Use os recursos descritos em Tabela 10 na página 26	Nenhuma

Tabela 8. Parâmetros de instalação silenciosa do Proteção de Dados para VMware (continuação)

Parâmetro	descrição	Valor padrão
<b>GUI_MODE</b>	Para proteger dados em um ambiente vSphere, especifique <b>GUI_MODE=vcenter</b> . Esse parâmetro instala o GUI do Data Protection for VMware vSphere. Essa GUI integra o produto com o cliente VMware vSphere para fazer backup, restaurar e gerenciar VMs em um ambiente VMware vCenter. Inclui o Interface da linha de comandos do Data Protection for VMware. É possível instalar somente um GUI do Data Protection for VMware vSphere em uma máquina. Como resultado, diversas GUIs do Proteção de Dados para VMware vSphere não são permitidas na mesma máquina. vcenter é o valor padrão quando <b>GUI_MODE</b> for especificado.	vcenter
<b>VCENTER_HOSTNAME</b>	O nome completo do domínio ou endereço IP do vCenter Server. Este recurso é necessário quando <b>GUI_MODE=vcenter</b> for especificado.	Nenhuma
<b>VCENTER_USERNAME</b>	O ID do usuário do vCenter. Este ID do usuário deve ser um administrador do VMware que possui permissão para registrar e cancelar o registro de extensões. Este recurso é necessário quando <b>GUI_MODE=vcenter</b> for especificado.	Nenhuma
<b>VCENTER_PASSWORD</b>	A senha do vCenter. Este recurso é necessário quando <b>GUI_MODE=vcenter</b> for especificado.	Nenhuma
<b>DIRECT_START</b>	(Apenas vSphere) Para acessar a GUI do Data Protection for VMware vSphere em um navegador da web, especifique <b>DIRECT_START=1</b> . O GUI do Data Protection for VMware vSphere é acessado por meio de um marcador de URL para o servidor da web da GUI. Se não desejar acessar a GUI do Data Protection for VMware vSphere em um navegador da web, especifique <b>DIRECT_START=0</b> .	1 <b>Importante:</b> Após a conclusão da instalação, o valor <b>DIRECT_START</b> não pode ser alterado, exceto pela reinstalação do produto.
<b>REGISTER_EXTENSION</b>	(somente vSphere) Para acessar a GUI do Proteção de Dados para VMware vSphere como uma extensão no vSphere Web Client, especifique <b>REGISTER_EXTENSION=1</b> .	0
<b>DB_PORT</b>	O número da porta TCP/IP para o banco de dados Derby.	1527
<b>WC_DEFAULTHOST</b>	O protocolo HTTP para o servidor da web da GUI.	9080
<b>WEBSERVER_SECUREPORT</b>	O protocolo HTTPS para o servidor da web da GUI.	9081

Tabela 9. Recursos de instalação silenciosa do Proteção de Dados para VMware

Recurso	descrição	Instalado por padrão?
shell	Interface da linha de comandos do agente de recuperação  Interface da linha de comandos que é usada para operações de montagem (RecoveryAgentShell.exe).	Sim
LAP	Licença do Proteção de Dados para VMware	Sim
TSMLicence	Arquivos de ativação do Data Protection for VMware  Permite que o IBM Spectrum Protect execute os tipos de backup a seguir: <ul style="list-style-type: none"> <li>• Backup incremental contínuo incremental</li> <li>• Backup incremental contínuo completo</li> </ul> Se você transferir cargas de trabalho de backup, esse arquivo deverá ser instalado no Servidor de Backup vStorage.	Sim
documents	Arquivo leia-me	Sim
gui	GUI do Data Protection for VMware vSphere	No

Use os seguintes parâmetros do movedor de dados com os recursos da instalação silenciosa:

Tabela 10. Parâmetros da instalação silenciosa do movedor de dados

Parâmetro	descrição	Valor padrão
<b>BackupArchiveGUI</b>	GUI do movedor de dados do IBM Spectrum Protect	Nenhuma
<b>BackupArchiveWeb</b>	Web client do movedor de dados do IBM Spectrum Protect	Nenhuma
<b>Api64Runtime</b>	Tempos de execução da API do IBM Spectrum Protect	Nenhuma
<b>AdministrativeCmd</b>	Linha de comandos administrativos do IBM Spectrum Protect	Nenhuma

## Sobre Esta Tarefa

**Restrição:** Todos os recursos são instalados em seu local padrão. Para localizar os diretórios de instalação padrão para os componentes, consulte os subtópicos em “Componentes Instaláveis” na página 1.

## Procedimento

Para instalar o Proteção de Dados para VMware, conclua as etapas a seguir a partir do diretório em que você extraiu o pacote:

1. Abra um prompt de comandos e vá até o local do arquivo spinstall.exe para obter o componente que deseja instalar.

2. Especifique quais recursos serão instalados.

O exemplo a seguir instala o agente de recuperação, o driver de dispositivo e a interface de linha de comando do agente do IBM Spectrum Protect:

```
spinstall.exe ISFeatureInstall=TSM4VE  
ComponentsToInstallVe=mount,mountdriver,shell  
REBOOT=ReallySuppress SUITE_MODE=1 /silent
```

O exemplo a seguir instala um subconjunto do Proteção de Dados para VMware e recursos do movedor de dados:

```
spinstall.exe ISFeatureInstall=Client,TSM4VE  
/silent  
ComponentsToInstallBa=BackupArchiveGUI,BackupArchiveWeb,Api64Runtime  
ComponentsToInstallVe=LAP,TSMLicence,documents,gui SUITE_MODE=1 REBOOT=ReallySuppress  
GUI_MODE=vcenter VCENTER_HOSTNAME=host_name  
VCENTER_USERNAME=user_name VCENTER_PASSWORD=password  
DIRECT_START=1
```

O exemplo a seguir instala todos os recursos do movedor de dados e do Proteção de Dados para VMware:

```
spinstall.exe /silent SUITE_MODE=1  
REBOOT=ReallySuppress  
GUI_MODE=vcenter VCENTER_HOSTNAME=host_name VCENTER_USERNAME=user_name  
VCENTER_PASSWORD=password DIRECT_START=1
```

3. Opcional: Após a instalação do driver de dispositivo, é necessário reiniciar o sistema.

**Nota:** A mensagem a seguir será exibida na primeira vez que você montar um volume:

```
O Driver de Volume Virtual não foi registrado ainda. O Recovery Agent pode registrar  
o driver agora. Durante o registro, um aviso do Microsoft Windows Logo  
poderá  
ser exibido.  
Aceite esse aviso para permitir a conclusão do registro.  
Deseja  
registrar o Driver de Volume Virtual agora?
```

Deve-se registrar o Driver de volume virtual para continuar com as operações do agente de recuperação.

**Tarefas relacionadas:**

“Desinstalando o Proteção de Dados para VMware for Windows em modo silencioso” na página 37

## Instalando o Proteção de Dados para VMware nos sistemas Linux no modo silencioso

É possível customizar quais recursos do Proteção de Dados para VMware instalar silenciosamente em um sistema operacional Linux.

### Antes de Iniciar

Antes de instalar o Proteção de Dados para VMware, assegure-se de atender aos requisitos a seguir:

- Assegure-se de que o ID do usuário tenha o nível de permissão necessário e de que as portas de comunicação necessárias estejam abertas antes de continuar.

- O processo de instalação cria o usuário `tdpvmware`. Você deve emitir todos os comandos `vmcli` como o usuário `tdpvmware` e com o ID do usuário raiz.
- O X Window Server é necessário ao instalar no modo do console.
- Assegure-se de ter revisado os requisitos a seguir:
  - “Requisitos do Sistema” na página 11
  - “Permissões de Instalação Necessárias” na página 12
  - “Portas de Comunicação Necessárias” na página 13

## Sobre Esta Tarefa

O Proteção de Dados para VMware fornece os seguintes recursos de instalação silenciosa para sistemas operacionais Linux:

*Tabela 11. Recursos de instalação silenciosa do Proteção de Dados para VMware*

Recurso	descrição	Instalado por padrão?
Docs	Arquivo leia-me	Sim
TDPVMwareDM	<p>A instalação desse recurso inclui o arquivo de ativação.</p> <p>Permite que o IBM Spectrum Protect execute os tipos de backup a seguir:</p> <ul style="list-style-type: none"> <li>• Backup incremental periódico da MV</li> <li>• Backup incremental contínuo da MV completa</li> <li>• Backup incremental contínuo incremental da MV</li> </ul> <p>Se você transferir cargas de trabalho de backup, esse arquivo deverá ser instalado no Servidor de Backup vStorage.</p>	Sim
TDPVMwareGUI	<p>GUI do Data Protection for VMware vSphere.</p> <p><b>Nota:</b> Inclui, também, a instalação do arquivo de ativação.</p>	Não

Use os seguintes parâmetros do Proteção de Dados para VMware com os recursos de instalação silenciosa:

*Tabela 12. Parâmetros de instalação silenciosa do Proteção de Dados para VMware para o arquivo `installer.properties`*

Parâmetro	descrição	Valor padrão
<b>VCENTER_HOSTNAME</b>	O nome completo do domínio ou endereço IP do vCenter Server.	Nenhuma
<b>VCENTER_USERNAME</b>	O ID do usuário do vCenter. Este ID do usuário deve ser um administrador do VMware que possui permissão para registrar e cancelar o registro de extensões.	Nenhuma
<b>VCENTER_PASSWORD</b>	A senha do vCenter.	Nenhuma

Tabela 12. Parâmetros de instalação silenciosa do Proteção de Dados para VMware para o arquivo *installer.properties* (continuação)

Parâmetro	descrição	Valor padrão
<b>DIRECT_START</b>	(Apenas vSphere) Para acessar o GUI do Data Protection for VMware vSphere em um navegador da web, especifique <b>DIRECT_START=YES</b> . O GUI do Data Protection for VMware vSphere é acessado por meio de um marcador de URL para o servidor da web da GUI. Se não desejar acessar a GUI do Data Protection for VMware vSphere em um navegador da web, especifique <b>DIRECT_START=NO</b> .	YES <b>Importante:</b> Após a conclusão da instalação, o valor <b>DIRECT_START</b> não pode ser alterado, exceto pela reinstalação do produto.
<b>USERNAME</b>	Nome de usuário. Um perfil para esse nome de usuário é criado em /home/<username>/tdpvmware/config.	tdpvmware
<b>REGISTER_EXTENSION</b>	(somente vSphere) Para acessar a GUI do Proteção de Dados para VMware vSphere como uma extensão no vSphere Web Client, especifique <b>REGISTER_EXTENSION=1</b> .	0
<b>VMCLI_DB_PORT</b>	O número da porta TCP/IP para o Banco de Dados Derby.	1527
<b>WC_defaulthost</b>	O protocolo HTTP para o servidor da web da GUI.	9080
<b>WebServer_Https</b>	O protocolo HTTPS para o servidor da web da GUI.	9081
<b>Keystore_Password</b>	A senha do keystore para o servidor da web da GUI. A senha deve ter, no mínimo, seis caracteres válidos (a-z A-Z 0-9).	Nenhuma
<b>SSL_Certificate</b>	O processo de instalação gera um certificado SSL autoassinado. Insira o número de anos para manter este certificado SSL ativo.	10

## Procedimento

Para instalar o Proteção de Dados para VMware, conclua as seguintes etapas a partir do diretório em que o pacote de instalação foi extraído:

1. Abra o arquivo *path../Linux/DataProtectionForVMware/installer.properties* e remova o comentário da seguinte entrada para aceitar a licença (em que *path* é a pasta de instalação):  

```
LICENSE_ACCEPTED=TRUE
```
2. Escolha um dos métodos a seguir para instalar os componentes do Proteção de Dados para VMware:
  - Para uma instalação padrão, abra a pasta CD/Linux/DataProtectionForVMware e insira o comando a seguir:  

```
./install-Linux.bin -i silent -LICENSE_ACCEPTED=true
```
  - Para uma instalação customizada, conclua as etapas a seguir:
    - a. Edite o arquivo *installer.properties* com os valores apropriados:

- 1) Especifique **INSTALL\_MODE=Custom**. Assegure-se de que o sinal de número (Nº) seja removido dessa instrução.
  - 2) Especifique os recursos a serem instalados com a opção **CHOSEN\_INSTALL\_FEATURE\_LIST**. Por exemplo, todos os recursos são instalados com o valor a seguir:  
`CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI`
  - 3) Especifique os parâmetros `installer.properties` conforme descrito em Tabela 12 na página 28.
- b. Na pasta `CD/Linux/DataProtectionForVMware`, emita o comando a seguir:  
`./install-Linux.bin -i silent -f installer.properties`

## Executando as primeiras etapas após instalar o Proteção de Dados para VMware

Após instalar o Proteção de Dados para VMware, prepare-se para a configuração. Usar o assistente de configuração é o método preferencial de configurar o Proteção de Dados para VMware.

### Planilha de configuração

Use essa planilha para registrar informações necessárias, ao configurar e administrar o Proteção de Dados para VMware. A planilha é destinada a ajudá-lo a se lembrar dos valores especificados após a configuração.

Tabela 13. Planilha de configuração do Proteção de Dados para VMware

Item	Seu valor	Notas
<b>Informações do servidor IBM Spectrum Protect</b>		
Endereço do servidor IBM Spectrum Protect		
Porta do servidor IBM Spectrum Protect		
ID/senha de administrador do servidor IBM Spectrum Protect		
Porta de administrador do servidor IBM Spectrum Protect		
<b>Opções de definição de nó</b>		
Prefixo a ser incluído nos nós		
Domínio de política a ser usado ao registrar novos nós		
Nome/senha do nó do vCenter		
Nome/senha do nó da VMCLI		
Senhas/nós do nó do datacenter  <b>Lembre-se:</b> É possível criar diversos nós do datacenter.		O nome do nó do datacenter consiste no prefixo especificado, seguido por um caractere de sublinhado, seguido pelo nome do datacenter.  Por Exemplo: <i>nodePrefix_datacenterName</i>
Nomes/senhas do nó do movedor no servidor de backup do vStorage  <b>Lembre-se:</b> É possível criar diversos nós do movedor de dados.		O nó do movedor de dados consiste no nome do nó do datacenter, seguido por um caractere de sublinhado, seguido por DM.  Por exemplo: <i>datacenterNodename_DM</i>



Tabela 13. Planilha de configuração do Proteção de Dados para VMware (continuação)

Item	Seu valor	Notas
Nomes/senhas do nó do movedor em servidores remotos  <b>Lembre-se:</b> É possível criar diversos nós do movedor de dados que não estão no servidor de backup do vStorage.		
Nó do proxy de montagem  O nó do proxy de montagem será usado ao restaurar os dados.	Windows:  Linux:	

## Acessando o GUI do Data Protection for VMware vSphere

Use o GUI do Data Protection for VMware vSphere para fazer backup, restaurar e gerenciar máquinas virtuais em um ambiente do VMware vCenter.

### Antes de Iniciar

Antes de poder acessar o GUI do Data Protection for VMware vSphere, durante a instalação, deve-se ter selecionado a opção para proteger seus dados em um ambiente do vSphere.

### Procedimento

- Se você tiver selecionado a opção **Ativar o acesso à GUI por um navegador da web** durante a instalação, será possível acessar o GUI do Data Protection for VMware vSphere a partir do navegador:
  1. Abra um navegador da web e insira a URL a seguir:  
`https://hostname:port/TsmVMwareUI`  
 em que:
    - *hostname* é o nome do sistema em que o GUI do Data Protection for VMware vSphere está instalado
    - *port* é o número da porta através da qual a GUI do vSphere é acessível. O número da porta padrão é 9081.
  2. Efetue login usando o ID do usuário e a senha do vCenter.
- Se você não tiver selecionado a opção **Ativar o acesso à GUI por um navegador da web** durante a instalação, será possível acessar o GUI do Data Protection for VMware vSphere concluindo as etapas a seguir:
  1. Abra o VMware vSphere Client e efetue login com o ID do usuário e a senha do vCenter.
  2. No painel Soluções e Aplicativos do vSphere Client, clique no ícone GUI do Data Protection for VMware vSphere.

---

## Fazendo Upgrade do Proteção de Dados para VMware

É possível fazer upgrade do Proteção de Dados para VMware a partir de uma versão anterior do software. O upgrade do Proteção de Dados para VMware também requer o upgrade de outros componentes.

Consulte o IBM Spectrum Protect Snapshot for VMware Instalação e Guia do Usuário ao trabalhar com este produto.

Para compatibilidade com versões anteriores, consulte a nota técnica 1648031.

## Fazendo upgrade do Proteção de Dados para VMware

Este procedimento documenta como fazer upgrade para o Proteção de Dados para VMware V8.1.0.

### Antes de Iniciar

**Importante:** Esse procedimento de upgrade se aplica a um sistema que não tem o IBM Spectrum Protect Snapshot for VMware instalado.

Você deve ter privilégios de administrador para atualizar o Proteção de Dados para VMware.

As atualizações para o GUI do Data Protection for VMware vSphere existente são processadas desta maneira:

- É feito backup dos arquivos de parâmetro antes que o processo de upgrade do GUI do Data Protection for VMware vSphere seja iniciado.
- São usados os mesmos números de Porta do Banco de Dados Derby e Porta Base Padrão do WebSphere Application Server.
- **Linux** Os valores no perfil (vmcliprofile) são usados para o Interface da linha de comandos do Data Protection for VMware.

### Restrição:

- **Windows** Quando o IBM Spectrum Protect for Virtual Environments foi instalado em um local não padrão, o processo de upgrade instalou recursos do IBM Spectrum Protect for Virtual Environments V8.1.0 no diretório de instalação padrão. Não é possível fazer upgrade para um local não padrão. Consulte os subtópicos no “Componentes Instaláveis” na página 1 para os diretórios de instalação padrão para cada recurso.
- **Linux** **Windows** O processo de upgrade não instala novos componentes.  
Por exemplo, se a versão anterior tiver apenas a GUI do agente de recuperação instalada, o procedimento de upgrade não instalará a interface da linha de comandos do agente de recuperação. Nesse cenário, você deve executar o programa de instalação novamente e, em seguida, selecionar o componente ausente a ser instalado.
- **Linux** A versão do agente de recuperação no Linux deve ser a mesma do agente de recuperação no proxy do Windows. Portanto, se você atualizar o agente de recuperação no Linux, também deverá atualizar a versão do agente de recuperação no proxy do Windows.

### Procedimento

Para atualizar o Proteção de Dados para VMware, execute as seguintes etapas:

1. Pare quaisquer componentes e serviços do Proteção de Dados para VMware que estejam em execução.
2. Desmonte quaisquer volumes virtuais montados. É possível usar a interface da linha de comandos ou a GUI do agente de recuperação (comando **mount del**) para desmontar os volumes.
3. Se o sistema para o qual você está fazendo upgrade tiver o movedor de dados do GUI do Data Protection for VMware vSphere e do IBM Spectrum Protect instalado, instale o movedor de dados V8.1.0. Siga as instruções em “Instalando os componentes do Proteção de Dados para VMware em sistemas Windows” na página 20.

**Nota:** Linux Se o movedor de dados V6.x estiver instalado, você deverá desinstalá-lo antes de instalar o V8.1.0. Siga as instruções em Desinstalando o cliente do IBM Spectrum Protect Linux x86\_64

4. Faça download do pacote de código.
5. Na pasta em que salvou o pacote de códigos, inicie o processo de upgrade:
  - a. Windows Execute o arquivo spinstall.exe.
  - b. Linux Execute o arquivo install-Linux.bin.

Uma mensagem exibe este texto: 0 Data Protection for VMware Existente será atualizado.

Se confirmar o upgrade, o instalador atualizará os arquivos. É possível instalar somente um GUI do Data Protection for VMware vSphere em uma máquina. Como resultado, diversos GUI do Data Protection for VMware vSpheres não são permitidos na mesma máquina.

## Atualizando o Proteção de Dados para VMware em um Sistema Windows de 64 bits no Modo Silencioso

É possível atualizar silenciosamente o Proteção de Dados para VMware em um sistema operacional de 64 bits suportado.

### Antes de Iniciar

Quando o Proteção de Dados para VMware V6.x foi instalado em um local não padrão, o processo de upgrade silencioso instalou recursos do Proteção de Dados para VMware V8.1.0 no diretório de instalação padrão. Não é possível fazer upgrade silenciosamente para um local não padrão. Consulte os subtópicos na seção do “Componentes Instaláveis” na página 1 para os diretórios de instalação padrão para cada recurso.

### Procedimento

Para atualizar o Proteção de Dados para VMware, execute as seguintes etapas:

1. Pare quaisquer componentes do Proteção de Dados para VMware que estiverem em execução.
2. Desmonte quaisquer volumes virtuais montados. É possível usar a interface da linha de comandos ou a GUI do agente de recuperação (comando **mount del**) para desmontar os volumes.
3. Desmonte quaisquer volumes virtuais montados. É possível usar a interface da linha de comandos ou a GUI do agente de recuperação (comando **mount del**) para desmontar os volumes.
4. Faça download do pacote de código.

5. Na pasta do Proteção de Dados para VMware, acesse a pasta X64.
6. Em uma janela de prompt de comando, digite o seguinte comando:
 

```
spinstall.exe /s /v"/qn
REBOOT=ReallySuppress"
```

## Atualizando o Proteção de Dados para VMware em um Sistema Linux no Modo Silencioso

É possível atualizar silenciosamente o Proteção de Dados para VMware em um sistema operacional Linux suportado.

### Sobre Esta Tarefa

Use os parâmetros do Proteção de Dados para VMware a seguir com o recurso de instalação silenciosa:

*Tabela 14. Parâmetros de upgrade de instalação silenciosa do Proteção de Dados para VMware*

Parâmetro	descrição	Valor padrão
<b>VCENTER_HOSTNAME</b>	O nome completo do domínio ou endereço IP do vCenter Server.	Nenhum
<b>VCENTER_USERNAME</b>	O ID do usuário do vCenter. Este ID do usuário deve ser um administrador do VMware que possui permissão para registrar e cancelar o registro de extensões.	Nenhuma
<b>VCENTER_PASSWORD</b>	A senha do vCenter.	Nenhuma
<b>DIRECT_START</b>	Para acessar o GUI do Data Protection for VMware vSphere em um navegador da web, especifique <b>DIRECT_START=YES</b> . O GUI do Data Protection for VMware vSphere é acessado por meio de um marcador de URL para o servidor da web da GUI. Se não desejar acessar a GUI do Data Protection for VMware vSphere em um navegador da web, especifique <b>DIRECT_START=NO</b> .	YES <b>Importante:</b> Após o upgrade ser concluído, o valor de <b>DIRECT_START</b> não pode ser mudado, exceto pela reinstalação do produto.

### Procedimento

Para atualizar o Proteção de Dados para VMware, execute as seguintes etapas:

1. Certifique-se de não haver backup ativo, restauração ou sessões de montagem.
2. Certifique-se de que qualquer GUI do GUI do Data Protection for VMware vSphere ou do agente de recuperação existente esteja fechada.
3. Faça download do pacote de código.
4. Na pasta do Proteção de Dados para VMware, acesse a pasta do Linux.
5. A partir de uma janela de prompt de comandos, insira o comando `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` com os parâmetros preferenciais.

Por Exemplo:

```
./install-Linux.bin -i silent -LICENSE_ACCEPTED=true
-VCENTER_HOSTNAME=hostname -VCENTER_USERNAME=username
-VCENTER_PASSWORD=password
-DIRECT_START=yes -REGISTER_EXTENSION=yes
```

---

## Desinstalando o Proteção de Dados para VMware

O processo de desinstalação do Proteção de Dados para VMware é o mesmo para uma nova instalação e para uma versão com upgrade.

### Desinstalando o Proteção de Dados para VMware nos sistemas Windows

Desinstale os componentes do Proteção de Dados para VMware e remova arquivos e diretórios de um sistema Windows.

#### Antes de Iniciar

Para assegurar uma desinstalação bem-sucedida, use a orientação a seguir:

- Se outros hosts da GUI da web do Proteção de Dados para VMware usarem o Extensão do IBM Spectrum Protect, não cancele o registro da extensão do Web client.
- Quando você desinstala o Extensão do IBM Spectrum Protect de um ambiente do VMware vSphere 5.5, apenas os rótulos e descrições de privilégios associados são removidos. Os privilégios reais permanecem instalados. Esse problema é uma limitação conhecida do VMware. Para obter mais informações, consulte o artigo de base de conhecimento do VMware a seguir: <http://kb.vmware.com/kb/2004601>.
- O Arquivo de Ativação do Proteção de Dados para VMware não é removido após o produto ser desinstalado.

#### Sobre Esta Tarefa

Os arquivos de propriedade e de configuração estarão localizados no diretório C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\config após a conclusão da desinstalação.

#### Procedimento

1. Pare quaisquer componentes do Proteção de Dados para VMware que estiverem em execução.
2. Desmonte quaisquer volumes virtuais montados. É possível usar a interface da linha de comandos ou a GUI do agente de recuperação (comando **mount del**) para desmontar os volumes.
3. Clique em **Iniciar > Painel de Controle > Programas e recursos > Desinstalar um programa**.
  - Se você tiver instalado o Proteção de Dados para VMware com o Instalador do Conjunto, selecione Data Protection for VMware suite e clique em **Desinstalar**.
  - Se você instalou o movedor de dados como parte da instalação do VE, será necessário remover manualmente a entrada IBM Spectrum Protect JVM de programas e recursos.

Essa ação desinstala o programa do Proteção de Dados para VMware do Windows. Ela também remove serviços que são associados ao Agente de recuperação, ao servidor da web e à interface da linha de comandos do Data Protection for VMware. Entretanto, essa ação não remove arquivos de log, serviços do movedor de dados e do proxy de montagem ou outros itens que foram criados quando você configurou ou usou o Proteção de Dados para VMware. Deixar esses artefatos no disco não será um problema, se desejar reinstalar o Proteção de Dados para VMware no futuro. No entanto, se desejar

4. Remova os arquivos e diretórios do Proteção de Dados para VMware a seguir do sistema de arquivos. Abra um prompt de comandos do administrador e conclua as etapas a seguir:

- Emita os seguintes comandos:

b. Acesse o diretório C:\Program Files (x86)\Common Files\Tivoli\. Por exemplo:

**Nota:** O comando a seguir exclui todos os arquivos de propriedade e de configuração que foram salvos após a desinstalação.

c. Acesse o diretório C:\ProgramData. Por exemplo:

Emita os seguintes comandos:

d. Acesse o diretório C:\ProgramData\Tivoli\TSM. Por exemplo:

Remova os arquivos a seguir se eles estiverem em seu sistema:

Emita o seguinte comando:

5. Pare qualquer componente do movedor de dados que esteja executando.

6. Exclua qualquer backup existente na máquina virtual emitindo o comando **delete backup** do movedor de dados. Por exemplo, para excluir o backup ativo de uma máquina virtual que é denominada vm1, emita o comando a seguir:

Para excluir uma ou mais versões de backup de uma máquina virtual que é denominada `vm_test.`, emita o comando a seguir:

7. Insira os comandos a seguir. É possível usar o comando **dsmcutil list** para exibir qualquer serviço do movedor de dados que esteja instalado.

- Se necessário, substitua `c:\program files\tivoli` pela pasta de instalação correta.

- 36 IBM Spectrum Protect for Virtual Environments: Proteção de Dados para VMware

**Importante:** Assegure-se de remover o TSM Remote Client Agent na Etapa 3b antes de remover o TSM Client Acceptor na etapa 3c. Caso contrário, o TSM Client Acceptor (etapa 3c) não poderá ser removido.

c. `dsmcutil remove /name:"TSM Client Acceptor"`

## O que Fazer Depois

Verifique se todos os componentes foram removidos do sistema.

## Desinstalando o Proteção de Dados para VMware for Windows em modo silencioso

É possível desinstalar silenciosamente o Proteção de Dados para VMware em um sistema operacional Windows.

### Sobre Esta Tarefa

Os arquivos de propriedade e de configuração estarão localizados no diretório `C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\config` após a conclusão da desinstalação.

### Procedimento

Para desinstalar o Proteção de Dados para VMware, execute as seguintes etapas:

1. Pare quaisquer componentes do Proteção de Dados para VMware que estiverem em execução.
2. Desmonte quaisquer volumes virtuais montados. É possível usar a interface da linha de comandos ou a GUI do agente de recuperação (comando **mount del**) para desmontar os volumes.
3. Em uma janela de prompt de comandos, use o comando **cd** para alterar para uma das seguintes pastas:
  - Para customizar a operação de desinstalação, acesse a pasta `X64`.
  - Para desinstalar o Proteção de Dados para VMware com o instalador do Conjunto, acesse `<extract folder>TSM4VE_WIN`.
4. Na janela de prompt de comandos, execute o seguinte comando:
  - Para uma operação de desinstalação customizada, selecione a partir dos seguintes comandos:
    - Insira este comando para desinstalar o Proteção de Dados para VMware e cancelar o registro do GUI do Data Protection for VMware vSphere:  

```
spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL  
VCENTER_HOSTNAME=<vCenter hostname or IP>  
VCENTER_USERNAME=<vCenter user name>  
VCENTER_PASSWORD=<vCenter password>"
```
  - Para desinstalar todos os recursos com o instalador do Suite, insira o seguinte comando:  

```
spinstall.exe /silent /remove
```
5. Reinicie o sistema após a conclusão da desinstalação.

## Desinstalando o Proteção de Dados para VMware em um sistema Linux

É possível desinstalar o Proteção de Dados para VMware em um sistema operacional Linux suportado.

### Sobre Esta Tarefa

Quando você desinstala o Proteção de Dados para VMware em um sistema Linux, por padrão, o tipo de desinstalação é o mesmo processo do tipo de instalação original. Para usar um processo de desinstalação diferente, especifique o parâmetro correto. Por exemplo, se você usou um processo de instalação silenciosa, será possível usar o assistente de instalação para desinstalar especificando o parâmetro `-i swing`. Execute o processo de desinstalação como o usuário raiz. O perfil do usuário raiz deve ser originado. Se você usar o comando `su` para alternar para root, use o comando `su -` para originar o perfil root.

Quando o processo de desinstalação começar a remover os arquivos de programas, o cancelamento do processo de desinstalação não retornará o sistema para um estado limpo. Essa situação poderá fazer com que a tentativa de reinstalação falhe. Como resultado, limpe o sistema concluindo as tarefas descritas em “Removendo Manualmente o Proteção de Dados para VMware a Partir de um Sistema Linux” na página 39.

Para desinstalar o Proteção de Dados para VMware, execute as seguintes etapas:

### Procedimento

1. Altere para o diretório do programa de desinstalação. O caminho a seguir é o local padrão para o programa de desinstalação: `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`
2. Dependendo do tipo de instalação, use um dos seguintes métodos para desinstalar o Proteção de Dados para VMware:

**Nota:** Os comandos neste procedimento devem ser inseridos em uma linha. Esses exemplos mostram duas linhas para acomodar a formatação de página.

- Para usar o assistente de instalação para desinstalar o Proteção de Dados para VMware, insira este comando:  
`./Uninstall_Tivoli_Data_Protection_for_VMware -i swing`
- Para usar o console para desinstalar o Proteção de Dados para VMware, insira este comando:  
`./Uninstall_Tivoli_Data_Protection_for_VMware -i console`
- Para desinstalar silenciosamente o Proteção de Dados para VMware, insira este comando:  
`./Uninstall_Tivoli_Data_Protection_for_VMware -i silent  
-f uninstall.properties`

O arquivo `uninstall.properties` contém as informações de conexão do vCenter. Essas informações são necessárias para desinstalar o GUI do Data Protection for VMware vSphere.



## Removendo Manualmente o Proteção de Dados para VMware a Partir de um Sistema Linux

### About this task

Quando o Proteção de Dados para VMware não puder ser desinstalado usando o procedimento de desinstalação padrão, deve-se remover o Proteção de Dados para VMware manualmente do sistema, como descrito nestas etapas. Execute este processo como o usuário raiz.

### Procedure

1. Se você tiver instalado o GUI do Data Protection for VMware vSphere, remova seu pacote do banco de dados do gerenciador de pacote com este comando:

```
rpm -e TIVsm-TDPVMwarePlugin
```

2. Remova a API do IBM Spectrum Protect com este comando:

```
rpm -e TIVsm-API64  
gskssl64.linux.x86_64.rpm  
skcrypt64.linux.x86_64  
TIVsm-TDPVMwarePlugin.x86_64.rpm  
TIVsm-DPAPI.x86_64.rpm
```

3. Remova as entradas do produto do Deployment Engine:

- a. Emita este comando para visualizar uma lista de todas as entradas:

```
/usr/ibm/common/acs/bin/de_lsrootiu.sh
```

- b. Emite este comando para remover as entradas de unidades instaladas, relacionadas ao Proteção de Dados para VMware:

```
/usr/ibm/common/acs/bin/deleteRootIU.sh <UUID> <discriminant>
```

Assegure-se de ter removido as entradas de unidade:

```
FBJRE  
TDPVMwareGUI  
JavaHelp  
TDPVMwareDM
```

4. Faça o backup do arquivo de registro global (/var/.com.zerog.registry.xml). Após o backup do arquivo ter sido feito, remova todas as tags relacionadas ao Proteção de Dados para VMware.
5. Remova todos os arquivos no diretório de instalação (/opt/tivoli/tsm/tdpvmware). Além disso, remova qualquer atalho que estiver na área de trabalho.
6. Faça o backup de arquivos de log que estão no diretório /root que contenha o TDPVMware no nome do arquivo. Por exemplo, IA-TDPVMware-00.log ou IA-TDPVMware\_Uninstall-00.log. Remova esses arquivos de log depois que o seu backup for feito. Removendo-os, será possível visualizar qualquer erro emitido se o processo de instalação falhar novamente.
7. Tente instalar o produto novamente, conforme descrito em “Instalando o Proteção de Dados para VMware em sistemas Linux” na página 22.



---

## Capítulo 2. Configurando o Proteção de Dados para VMware

Esta seção fornece instruções para configurar o Proteção de Dados para VMware e iniciar serviços relacionados.

---

### Configurando uma nova instalação com o assistente

Use o assistente de configuração para a configuração inicial ou para concluir mudanças menores.

#### Antes de Iniciar

O sistema em que o Proteção de Dados para VMware está instalado deve ter conectividade de rede com os servidores a seguir:

- Servidor de Backup vStorage
- Servidor IBM Spectrum Protect
- vCenter Server

#### Sobre Esta Tarefa

Para configurar o ambiente do Proteção de Dados para VMware, conclua estas etapas:

#### Procedimento

1. Abra um navegador da web e insira o endereço do servidor da web da GUI.  
Por exemplo:  
`https://guihost.mycompany.com:9081/TsmVMwareUI/`
  - Em um ambiente vSphere, efetue login com o nome de usuário e a senha do vCenter.
2. Na janela Introdução, acesse a janela Configuração e clique em **Executar Assistente de Configuração**.
3. Siga as instruções em cada página do assistente até que a janela Resumo seja exibida. Revise as configurações e clique em **Confluir** para concluir a configuração e sair do assistente.  
  
**Dica:** As informações sobre cada página de configuração são fornecidas na ajuda online instalada com a GUI. Clique em **Saiba Mais** em qualquer uma das janelas da GUI para abrir a ajuda online e obter assistência de tarefa. Consulte o tópico *Executando o Assistente de Configuração*.
4. Verifique se os nós do movedor de dados estão configurados corretamente:
  - a. Clique na guia **Configuração** para visualizar a página Status da Configuração.
  - b. Na página Status de Configuração, selecione um nó do movedor de dados para visualizar suas informações de status na área de janela Detalhes do Status. Quando um nó exibir um aviso ou erro, clique nesse nó e use as informações na área de janela Detalhes do Status para resolver o problema. Em seguida, selecione o nó e clique em **Validar Nó Selecionado** para verificar se o problema é resolvido. Clique em **Atualizar** para um novo teste de todos os nós.

## Resultados

**Atalho:** Depois de concluir com êxito essa tarefa do assistente, nenhuma tarefa de configuração adicional será necessária para fazer backup dos dados da MV.

---

## Usando o bloco de notas para editar uma instalação existente

Use o bloco de notas Editar Configuração para editar definições de configuração existentes.

### Antes de Iniciar

O bloco de notas de Configuração de Edição fornece as tarefas a seguir para uma configuração existente:

- Configurar ou mudar o ID de administrador do IBM Spectrum Protect.
- Reconfigurar a senha ou desbloquear o nó VMCLI.
- (Ambiente vSphere) Inclua ou remova datacenters do VMware no domínio da GUI do Data Protection for VMware vSphere.
- Inclua ou remova os nós do proxy de montagem. Modifique uma senha para um nó do proxy de montagem existente.
- Inclua ou remova nós do movedor de dados. Modifique uma senha para um nó do movedor de dados existente.
- Ative a restauração de arquivo.
- Ative o suporte à identificação para um nó do movedor de dados.

### Sobre Esta Tarefa

Para editar uma configuração existente, conclua estas etapas:

### Procedimento

1. Abra um navegador da web e insira o endereço do servidor da web da GUI.  
Por exemplo:  
`https://guihost.mycompany.com:9081/TsmVMwareUI/`
  - Em um ambiente vSphere, efetue login com o nome do usuário e a senha do vCenter.
2. Na janela Introdução, acesse a janela Configuração e clique em **Configuração de Edição**.
3. Acesse a página relevante para sua tarefa de edição e siga as instruções. Você deve clicar em **OK** para salvar suas mudanças antes de continuar com outra página Definições de Configuração. Caso contrário, suas mudanças não entrarão em vigor.

**Importante:** As informações sobre cada página de configuração são fornecidas na ajuda online instalada com a GUI. Clique em **Saiba Mais** em qualquer uma das janelas da GUI para abrir a ajuda online e obter assistência de tarefa. Consulte o tópico *Editando uma Configuração Existente*.

## Resultados

As configurações atualizadas são exibidas na janela Configuração.

---

## Ativando o ambiente para operações de restauração de arquivo

### Windows

Quando o recurso de restauração de arquivo for ativado por um administrador, os proprietários de arquivo poderão restaurar arquivos sem assistência.

### Antes de Iniciar

Se você não verificou se todos os pré-requisitos foram atendidos, revise o tópico sobre pré-requisitos de restauração de arquivos no *IBM Spectrum Protect for Virtual Environments: guia do usuário do Proteção de Dados para VMware*.

### Sobre Esta Tarefa

Conclua estas etapas no sistema no qual o GUI do Data Protection for VMware vSphere está instalado.

### Procedimento

1. Inicie o GUI do Data Protection for VMware vSphere abrindo um servidor da web e inserindo o endereço do servidor da web da GUI. Por exemplo:

`https://<endereço do servidor da web da GUI>:9081/TsmVMwareUI/`

Efetue login com o ID do usuário e senha do vCenter.

2. A partir da janela Introdução, clique em **Configuração** e selecione uma das tarefas a seguir na lista Tarefas:
  - Se você estiver configurando um novo ambiente, conclua as etapas a seguir:
    - a. Selecione **Executar Assistente de Configuração do Cliente**.
    - b. Siga as instruções em cada página do assistente. Use a orientação a seguir para concluir a página Restauração de arquivo:
      - 1) Selecione a opção **Ativar restauração de arquivo**.
      - 2) Insira as informações de contato do administrador que são mostradas na interface de restauração de arquivo. Se não desejar fornecer informações de contato, desmarque a caixa de seleção.
      - 3) Se o ambiente contiver backups de máquinas virtuais do Windows, insira as credenciais do administrador de domínio do Windows. Caso contrário, limpe a caixa de seleção e não insira nenhuma credencial.

**Dica:** Uma operação de restauração de arquivo usa as credenciais de administrador de domínio para acessar compartilhamentos de rede de acesso na máquina virtual remota. Uma operação falhará quando o ambiente contiver backups de máquinas virtuais do Windows e nenhuma credencial, ou credencial incorreta, for inserida. Portanto, limpe essa caixa de seleção somente quando não houver backups de máquina virtual do Windows.

- 4) Clique na URL de interface de restauração de arquivo para verificar se a interface é acessível.

**Lembre-se:** Mantenha um registro da URL de interface de restauração de arquivo. O proprietário da máquina virtual guest acessa a interface de restauração de arquivo por meio dessa URL.

- 5) Clique em **OK** para salvar suas alterações.

- Se você estiver atualizando um ambiente existente, conclua as etapas a seguir:
  - a. Selecione **Editar configuração do TSM**.
  - b. Na página Restauração de arquivo, use a orientação a seguir:
    - 1) Selecione a opção **Ativar restauração de arquivo**.
    - 2) Insira as informações de contato do administrador que são mostradas na interface de restauração de arquivo. Se não desejar fornecer informações de contato, desmarque a caixa de seleção.
    - 3) Se o ambiente contiver backups de máquinas virtuais do Windows, insira as credenciais do administrador de domínio do Windows. Caso contrário, limpe a caixa de seleção e não insira nenhuma credencial.

**Dica:** Uma operação de restauração de arquivo usa as credenciais de administrador de domínio para acessar compartilhamentos de rede de acesso na máquina virtual remota. Uma operação falhará quando o ambiente contiver backups de máquinas virtuais do Windows e nenhuma credencial, ou credencial incorreta, for inserida. Portanto, limpe essa caixa de seleção somente quando não houver backups de máquina virtual do Windows.

- 4) Clique na URL de interface de restauração de arquivo para verificar se a interface é acessível.

**Lembre-se:** Mantenha um registro da URL de interface de restauração de arquivo. O proprietário da máquina virtual guest acessa a interface de restauração de arquivo por meio dessa URL.

- 5) Clique em **OK** para salvar suas alterações.

## Resultados

O ambiente está ativado para operações de restauração de arquivo. Os proprietários do arquivo podem restaurar seus arquivos usando a URL para acessar a interface de restauração de arquivo do IBM Spectrum Protect.

## Configurando operações de restauração de arquivos no Linux

Linux

Para ativar o recurso de restauração de arquivos quando o Proteção de Dados para VMware estiver instalado em um sistema Linux, deve-se configurar um ambiente adicional do Proteção de Dados para VMware em um sistema Windows.

### Sobre Esta Tarefa

Ao executar o Proteção de Dados para VMware em um ambiente Linux ou em conjunto com o IBM Spectrum Protect Snapshot for VMware, o recurso de restauração de arquivos deve ser instalado em um sistema Windows para ser ativado.

### Procedimento

1. Configure um servidor Windows separado a ser usado para o recurso de restauração de arquivos.
2. Instale o Proteção de Dados para VMware no sistema Windows. Aceite os valores padrão durante a instalação.

3. Ao configurar o Proteção de Dados para VMware no sistema Windows, use os seguintes nomes de nó:
  - a. Crie um nó do vCenter chamado VCENTER\_FR.
  - b. Crie um nó do VMCLI chamado VMCLI\_FR.
  - c. Reutilize o nó do datacenter do ambiente Linux.  
Por exemplo: DATACENTER.
  - d. Não crie um nó do movedor de dados. O recurso de restauração de arquivos não necessita de um nó do movedor de dados nesse cenário.
  - e. Crie o novo par de nós de proxy de montagem a seguir, chamados REMOTE\_FR\_MP\_WIN e REMOTE\_FR\_MP\_LNX.
4. Na página Restauração de arquivos no assistente de configuração, selecione a opção Ativar restauração de arquivos.
5. Para acessar a interface de restauração do arquivo, abra um navegador da web e insira a URL fornecida pelo administrador. Por Exemplo:  
https:\\hostname:9081\FileRestoreUI

em que hostname é o nome do host do sistema Windows no qual o Proteção de Dados para VMware está instalado.

## Resultados

O exemplo a seguir mostra os relacionamentos de nó do proxy no servidor IBM Spectrum Protect:

tsm: SERVER>q proxy

Nó de Destino	Nó do Agente
VCENTER	VMCLI DATACENTER
VCENTER_FR	VMCLI_FR DATACENTER
DATACENTER	VMCLI VMCLI_FR
	DATAMOVER1
	REMOTE_MP_WIN REMOTE_MP_LNX
	REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX

Os nós adicionais criados para ativar o recurso de restauração de arquivos têm o sufixo \_FR.

## Modificando opções para as operações de restauração de arquivo

### Windows

Para permitir que os administradores configurem e controlem o processamento de restauração para operações de restauração de arquivo, modifique as opções no arquivo frConfig.props.

### Sobre Esta Tarefa

Conclua estas etapas no sistema no qual o GUI do Data Protection for VMware vSphere está instalado.

### Procedimento

1. Acesse o diretório em que o arquivo frConfig.props está localizado. Por exemplo, abra um prompt de comandos e emita o comando a seguir:  
cd C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\tsmVmGUI

2. Abra o arquivo `frConfig.props` com um editor de texto no modo de administrador e modifique as opções, conforme necessário. Use as informações no “Opções de restauração de arquivo” para determinar quais opções modificar.
3. Salve suas mudanças e feche o arquivo `frConfig.props`.

## Resultados

As opções modificadas são aplicadas à interface de restauração de arquivo do IBM Spectrum Protect.

## Opções de restauração de arquivo

As opções `frConfig.props` controlam a configuração, o suporte e o processamento de restauração para operações de restauração de arquivo.

### **`enable_contact_info=false | true`**

Especifique se deve fornecer informações de contato de administrador que os proprietários do arquivo podem usar para obter suporte.

#### **`false`**

Os proprietários do arquivo não recebem informações de contato de administrador. Esse valor é padrão.

#### **`true`**

Os proprietários do arquivo recebem informações de contato de administrador.

Se você especificar **`enable_contact_info=true`**, deverá fornecer informações na opção **`contact_info`**.

### **`enable_filerestore=false | true`**

Especifique se os proprietários do arquivo podem restaurar seus arquivos a partir de uma máquina virtual com a interface de restauração de arquivo do IBM Spectrum Protect.

#### **`false`**

Os proprietários do arquivo não podem restaurar seus arquivos com a interface de restauração de arquivo do IBM Spectrum Protect. Esse valor é padrão.

#### **`true`**

Os proprietários do arquivo podem restaurar seus arquivos com a interface de restauração de arquivo do IBM Spectrum Protect.

### **`maximum_mount_points=num_mount_points`**

Especifique o número máximo de pontos de recuperação simultâneos que estão disponíveis para a conta do usuário. O valor mínimo é 1 ponto de recuperação. O valor máximo é 256 pontos de montagem. O valor padrão é 2 pontos de montagem.

**Dica:** Para evitar que uma máquina virtual seja montada várias vezes para operações de restauração simultâneas, configure essa opção com um valor baixo.

### **`mount_session_timeout_minutes=num_mins`**

Especifique a quantidade de tempo, em minutos, que uma restauração e o ponto de recuperação montado podem estar inativos antes de a sessão ser cancelada. Um cancelamento desmonta o ponto de recuperação. O valor máximo é 8 horas (480 minutos). O valor padrão é 30 minutos.



**Dica:** Para evitar que a sessão seja cancelada inesperadamente, aumente o número de minutos.

**restore\_info\_duration\_hours=num\_hrs**

Especifique a quantia de tempo, em horas, em que as informações sobre a atividade de restauração recente são retidas na interface de restauração de arquivo do IBM Spectrum Protect. Use a janela de atividade de restauração para visualizar informações de erro e tarefas concluídas recentemente. Essas informações fornecem uma maneira para localizar arquivos restaurados recentemente. O valor máximo é 14 dias (336 horas). O valor padrão é uma semana (168 horas).

**contact\_info=administrator information**

Forneça informações de contato de administrador que os proprietários do arquivo podem usar para obter suporte. As informações de contato são exibidas na interface do arquivo de restauração do IBM Spectrum Protect nos locais a seguir:

- Janela de login
- A área de janela Sobre no menu de ajuda
- O link de informações de suporte nas mensagens da interface

É possível sobrescrever as opções a seguir com o assistente de configuração ou o bloco de notas do GUI do Data Protection for VMware vSphere:

- **enable\_contact\_info**
- **enable\_filerestore**
- **contact\_info**

---

## Configurando a atividade de log para operações de restauração de arquivo

Para permitir que os administradores configurem e controlem como o conteúdo é formatado e registrado para as operações de restauração de arquivo, modifique as opções no arquivo FRLog.config.

### Antes de Iniciar

O arquivo FRLog.config é gerado a primeira vez que a interface de restauração de arquivo do IBM Spectrum Protect é acessada.

### Sobre Esta Tarefa

Conclua estas etapas no sistema no qual o GUI do Data Protection for VMware vSphere está instalado.

### Procedimento

1. Acesse o diretório em que o arquivo FRLog.config está localizado. Abra um prompt de comandos e emita o comando a seguir:  

```
cd Install_Directory\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\frGUI\
```
2. Abra o arquivo FRLog.config com um editor de texto no modo de administrador e modifique as opções, conforme necessário. Use as informações no “Opções de atividade do log de restauração de arquivos” na página 48 para determinar quais opções modificar.
3. Salve suas mudanças e feche o arquivo FRLog.config.
4. Reinicie o servidor da web da GUI:

- a. Clique em **Iniciar > Painel de Controle > Ferramentas Administrativas > Serviços**.
- b. Clique com o botão direito em **Serviço do Servidor da Web do Data Protection for VMware** e clique em **Reiniciar**.

## Resultados

As configurações são aplicadas ao conteúdo e ao formato de informações de criação de log para operações de restauração de arquivo.

## Opções de atividade do log de restauração de arquivos

As opções `FRLog.config` controlam o conteúdo e o formato das informações de criação de log para as operações de restauração de arquivos.

As seguintes opções de informações de log estão disponíveis para as tarefas de restauração de arquivos no arquivo `fr_gui.log`:

### **MAX\_LOG\_FILES=number**

Especifique o número máximo de arquivos `fr_gui.log` a serem retidos. O valor padrão é 8.

### **MAX\_LOG\_FILE\_SIZE=number**

Especifique o tamanho máximo do arquivo `fr_gui.log` em KBs. O valor padrão é 8192 KB.

As seguintes opções de informações de log estão disponíveis para os serviços de restauração de arquivos no arquivo `fr_api.log`. Estes são serviços de API internos, relacionados à atividade de restauração de arquivos:

### **API\_MAX\_LOG\_FILES=number**

Especifique o número máximo de arquivos `fr_api.log` a serem retidos. O valor padrão é 8.

### **API\_MAX\_LOG\_FILE\_SIZE=number**

Especifique o tamanho máximo do arquivo `fr_api.log` em KBs. O valor padrão é 8192 KB.

### **API\_LOG\_FILE\_NAME=API\_log\_file\_name**

Especifique o nome do arquivo de log da API. O valor padrão é `fr_api.log`.

### **API\_LOG\_FILE\_LOCATION=API\_log\_file\_name**

Especifique o local do arquivo de log da API. O local deve ser especificado com uma barra (/). O local padrão é `Install_Directory/IBM/tivoli/tsm/tdpvmware/webserver/usr/servers/veProfile/logs`.

### **FR.API.LOG=ON | OFF**

Especifique se deseja ativar a criação de log para serviços de restauração de arquivos.

- Para ativar a criação de log para serviços de restauração de arquivos, especifique **ON**. O valor padrão é **ON**.
- Para desativar a criação de log para serviços de restauração de arquivos, especifique **OFF**.

Para solucionar problemas que podem ser encontrados durante as operações de restauração de arquivo, consulte **Opções de rastreamento para restauração de arquivo**. Também são especificadas opções de rastreamento no arquivo `FRLog.config`.

---

## Configurando um nó do movedor de dados para suporte de identificação

Quando o suporte de identificação está ativado em um nó do movedor de dados, os administradores podem aplicar tags de proteção de dados a objetos de inventário no VMware vCenter.

### Antes de Iniciar

Certifique-se de que os seguintes requisitos sejam atendidos:

- O VMware vCenter Server deve estar na Versão 6.0 Atualização 1 ou mais recente.
- Para que o GUI do Data Protection for VMware vSphere funcione corretamente com suporte de identificação, assegure-se de que os seguintes requisitos sejam atendidos durante a instalação da GUI:

- Pelo menos um movedor de dados e o GUI do Data Protection for VMware vSphere devem estar instalados no mesmo servidor. Este nó do movedor de dados deve estar configurado para que as credenciais do servidor vCenter sejam salvas. É possível salvar as credenciais executando o assistente de configuração para salvar a senha do nó do movedor de dados, ou usando o comando **dsmc set password** na linha de comandos do movedor de dados.

Se você usar outros movedores de dados, em execução em máquinas virtuais ou máquinas físicas como movedores de dados adicionais, é possível instalá-los em outros servidores. Para suporte de identificação, todos esses movedores de dados também devem ser configurados com a opção `vmtagdatamover=yes`. Esses movedores de dados adicionais não requerem que o GUI do Data Protection for VMware vSphere esteja instalado no mesmo servidor para que eles trabalhem corretamente como movedores de nós baseados em identificação.

- **Linux** Para movedores de dados do Linux, certifique-se de especificar o diretório de instalação do movedor de dados e a biblioteca compartilhada `Java™ libjvm.so` na variável de ambiente `LD_LIBRARY_PATH`. O caminho para `libjvm.so` é usado para suporte à identificação quando você ativa a opção `vmtagdatamover` no movedor de dados. Para obter instruções, consulte *Configurando os nós do movedor de dados em um ambiente vSphere*.
- **Linux** Em sistemas operacionais Linux, o GUI do Data Protection for VMware vSphere deve ser instalado usando o nome de usuário padrão (`tdpvmware`).
- **Linux** Para os nós do movedor de dados do Linux, o arquivo de senha padrão (`/etc/adsm/TSM.PWD`) deve ser usado.

### Sobre Esta Tarefa

É possível usar tags de proteção de dados para configurar a política de backup de máquinas virtuais em objetos de inventário do VMware. Essas tags de proteção de dados são apresentadas como configurações que podem ser mudadas no Extensão do IBM Spectrum Protect. Para tags relacionadas a planejamentos, as máquinas virtuais devem estar em um conjunto de proteção protegido por um planejamento. Um conjunto de proteção consiste nas máquinas virtuais em um contêiner que está designado à tag `Schedule` (IBM Spectrum Protect).

## Procedimento

Use um dos métodos a seguir:

- Para configurar um *novο* movedor de dados para suporte de identificação no Windows usando o GUI do Data Protection for VMware vSphere, conclua as etapas a seguir:
  1. No sistema Windows no qual o GUI do Data Protection for VMware vSphere está instalado, inicie a GUI abrindo um navegador da web e inserindo o endereço do servidor da web da GUI. Por exemplo:  
`https://<GUI web server address>:9081/TsmVMwareUI/`

Efetue login com o ID do usuário e senha do vCenter.

2. Acesse a guia **Configuração** e selecione a ação **Editar configuração do IBM Spectrum Protect**.
3. Acesse a página Nós do movedor de dados do bloco de notas da configuração.
4. Inclua um nó do movedor de dados concluindo as etapas a seguir:
  - a. Para o nó do movedor de dados para o qual você deseja configurar suporte de identificação, selecione **Criar serviços** e, em seguida, selecione **Nó baseado em identificação**.
  - b. Para designar o nó baseado em tag como um nó do movedor de dados padrão, selecione **Movedor de Dados Padrão**. Um nó do movedor de dados padrão fará backup de quaisquer novas VMs incluídas em qualquer contêiner no datacenter, se o contêiner já estiver em um conjunto de proteção. O movedor de dados padrão também faz backup de quaisquer VMs no conjunto de proteção que não tenham a tag Data Mover designada.

**Dica:** Se você editar a configuração, incluir um novo nó do movedor de dados e selecionar esse novo movedor de dados para ser o movedor de dados padrão do datacenter e a opção `vmtagdefaultdatamover` estiver configurada em seus outros arquivos de opção do movedor de dados, deve-se editar manualmente os arquivos de opções do movedor de dados para os outros movedores de dados no datacenter para mudar o valor de `vmtagdefaultdatamover` para o movedor de dados recém-criado.

- c. Clique em **OK** para salvar suas alterações.  
As opções `vmtagdefaultdatamover` e `vmtagdefaultdatamover` (se configuradas) são incluídas no arquivo de opções do movedor de dados (`dsm.opt`).
- Para configurar um nó do movedor de dados Linux *novο* ou *existente* ou um nó do movedor de dados Windows *existente* para suporte de identificação:
    1. Inclua a opção `vmtagdatamover yes` no arquivo de opções do movedor de dados (`dsm.sys` para Linux e `dsm.opt` para Windows).
    2. Para designar o nó baseado em tag como um nó do movedor de dados padrão, inclua a opção `vmtagdefaultdatamover yes` ou `vmtagdefaultdatamover dm_name` no arquivo de opções do movedor de dados.




**Dica:** Se você editar a configuração, incluir um novo nó do movedor de dados e selecionar esse novo movedor de dados para ser o movedor de dados padrão do datacenter e a opção `vmtagdefaultdatamover` estiver configurada em seus outros arquivos de opção do movedor de dados, deve-se editar manualmente os arquivos de opções do movedor de dados

para os outros movedores de dados no datacenter para mudar o valor de `vmtagdefaultdatamover` para o movedor de dados recém-criado.

## Resultados

Após o nó do movedor de dados ser ativado para suporte de identificação, o movedor de dados consultará o inventário do VMware para obter informações de identificação ao executar um backup. O movedor de dados, então, faz backup das máquinas virtuais de acordo com as tags de proteção de dados configuradas. Se o nó do movedor de dados não for configurado para suporte de identificação, quaisquer tags de proteção de dados serão ignoradas durante uma operação de backup.

### Informações relacionadas:

-  `Vmtagdatamover`
-  `Vmtagdefaultdatamover`
-  Configurando políticas de backup

---

## Configurando seu ambiente para operações de restauração instantânea de máquina virtual completa

Configure uma rede iSCSI dedicada para operações de acesso instantâneo e restauração instantânea de máquina virtual completa.

### Antes de Iniciar

Use a documentação apropriada do VMware (ESXi ou vSphere) para determinar as etapas específicas a serem seguidas para a configuração do comutador virtual iSCSI e rede de máquina virtual. Embora diretrizes gerais sejam fornecidas, a documentação específica e as explicações de como incluir redes virtuais e comutadores virtuais estão fora do escopo da documentação do produto. No momento desta publicação, a documentação do VMware vSphere ESXi and vCenter 5.5 estará disponível em VMware ESXi and vCenter Server 5 Documentation. Os tópicos “Redes” contêm as informações para inclusão e configuração de comutadores virtuais e redes virtuais.

**Importante:** Essas definições de configuração são fornecidas para ajudar na configuração do ambiente VMware para operações de acesso instantâneo e restauração instantânea de máquina virtual completa eficientes. No entanto, como essas configurações se aplicam às tarefas de configuração de VMware e interfaces com o usuário de VMware, você deve consultar a documentação VMware apropriada para obter instruções detalhadas passo a passo.

### Sobre Esta Tarefa

Esse procedimento requer um adaptador iSCSI em cada host ESXi usado para operações de restauração instantânea. Use a documentação apropriada do VMware para configurar o adaptador. No momento desta publicação, os procedimentos a seguir estarão disponíveis em VMware ESXi and vCenter Server 5 Documentation.

- Para configurar um adaptador iSCSI de software, siga as instruções no procedimento “Configurar adaptadores iSCSI de software” do VMware.
- Para configurar um adaptador iSCSI de hardware, siga as instruções no procedimento “Configurando adaptadores iSCSI de hardware independentes” do VMware.

## 1. Configurando o software iSCSI no host ESXi

### Procedure

Esta tarefa configura o software iSCSI para uma configuração básica.

1. Efetue login no host ESXi a ser usado para operações de restauração instantânea.
2. Siga as instruções neste artigo VMware Knowledge Base até que o adaptador iSCSI seja ativado: <http://kb.vmware.com/kb/1008083>  
O IBM Spectrum Protect descobre automaticamente o servidor de destino iSCSI.
3. Verifique se o endereço IP do adaptador iSCSI (no host ESXi) é o mesmo endereço de sub-rede usado pelo movimentador de dados.
4. Verifique se a licença do Storage vMotion está ativada no host ESXi.

### What to do next

Após o software iSCSI ser configurado no host ESXi, instale e configure aplicativos no sistema movimentador de dados.

## 2. Instalando e configurando aplicativos no movimentador de dados

### Before you begin

Se o Recovery Agent V8.1.0 e o movedor de dados do IBM Spectrum Protect V8.1.0 estiverem instalados e configurados no sistema movedor de dados, inicie na Etapa 3.

### Procedure

Esta tarefa configura o sistema movimentador de dados com os aplicativos e as configurações para operações de restauração instantânea.

1. Instale o Recovery Agent V8.1.0 e o movedor de dados do IBM Spectrum Protect V8.1.0 no sistema movedor de dados.  
Na Etapa 4 do procedimento Instalando o Data Protection for VMware, selecione o tipo de instalação **Instalar um movedor de dados completo para proteção de aplicativo dentro do guest**.
2. Configure o movedor de dados.  
Siga as instruções em Configurando o movedor de dados.
3. Configure o endereço IP do servidor iSCSI:
  - a. Acesse o arquivo C:\Program Files\Tivoli\TSM\baclient\dsm.opt e especifique o seguinte parâmetro:  
VMISCSIServeraddress=<IP address of the network card on the data mover system that exposes the iSCSI targets.>

Se seu sistema movimentador de dados tiver mais de uma placa de rede, certifique-se de especificar a placa de rede correta para a rede iSCSI.

### What to do next

Após o sistema movimentador de dados ser configurado, estabeleça uma conexão entre a CLI do Recovery Agent e a GUI do Recovery Agent.

### 3. Configurando a conexão do Recovery Agent

#### Before you begin

A interface da linha de comandos (CLI) do Recovery Agent V7.1.x pode ser visualizada como uma API de linha de comandos para a GUI do Recovery Agent. É possível usar a CLI do Recovery Agent para comunicação com a GUI do Recovery Agent.

#### Procedure

Esta tarefa estabelece uma conexão entre a CLI do Recovery Agent e a GUI do Recovery Agent.

1. Inicie a CLI do Recovery Agent no sistema movimentador de dados.  
No menu **Iniciar do Windows**, clique em **Programas > IBM Spectrum Protect > IBM Spectrum Protect for Virtual Environments > IBM Spectrum Protect Recovery Agent**.
2. Na janela de prompt de comando, insira o seguinte comando:  

```
RecoveryAgentShell.exe -c set_connection mount_computer <IP address  
of the network card on the data mover system that exposes the iSCSI targets.>
```

Esse comando estabelece uma conexão entre a CLI do Recovery Agent e a GUI do Recovery Agent.

#### What to do next

Após estabelecer uma conexão, configure uma rede iSCSI dedicada.

### 4. Configurando uma rede iSCSI dedicada para o host ESXi e o movimentador de dados

#### Before you begin

Revise estas diretrizes antes de continuar com a próxima tarefa:

- Use uma rede iSCSI dedicada para operações de restauração instantânea.
- Cada host ESXi que é usado para operações de restauração instantânea deve ter uma segunda placa de rede física disponível. Essa segunda placa de rede é ligada ao adaptador iSCSI de software do respectivo host ESXi.
- O sistema movimentador de dados que é executado em uma máquina virtual deve ter uma segunda placa de rede disponível. Essa segunda placa de rede é ligada ao adaptador iSCSI de software do host ESXi.
- Cada host ESXi que é usado para operações de restauração instantânea deve ter um armazenamento de dados VMware secundário disponível. Esse armazenamento de dados provisório contém as informações de configuração e os dados da máquina virtual que são criados durante a operação.

#### Procedure

Esta tarefa configura uma rede iSCSI dedicada para o host ESXi e para o movimentador de dados que é executado em uma máquina virtual.

1. Efetue login no host ESXi a ser usado para operações de restauração instantânea.
2. Configure o comutador virtual para a rede iSCSI.  
Estas etapas usam *vSwitch1* para o comutador virtual.

- a. Selecione **VMkernel Network Adapter** para **Tipo de Conexão**.  
A rede iSCSI requer esse tipo de conexão.
  - b. Selecione **Criar um comutador padrão vSphere** para **Acesso à Rede VMkernel**.
  - c. Selecione **Rótulo da Rede** para **Configurações de Conexão do VMkernel**.  
Especifique um rótulo que indique se o *vSwitch1* e essa rede são para seu tráfego iSCSI.  
Por exemplo: *VMkernel iSCSI*.
  - d. Especifique um endereço IP e uma máscara de sub-rede para *vSwitch1* em **Configurações de Conexão IP do VMkernel**.  
Não altere os valores de **Máscara de Sub-rede** ou **Gateway Padrão VMkernel**.
  - e. Especifique a porta do kernel para a rede iSCSI operar.
3. Configure o comutador virtual para a rede de máquina virtual.  
Estas etapas usam *vSwitch0* para o comutador virtual.
    - a. Selecione **Máquina Virtual** para o **Tipo de Conexão**.
    - b. Selecione **Criar um comutador padrão vSphere** para o **Acesso de rede VMkernel**.
    - c. Acesse a guia **Propriedades do Grupo da Porta** e selecione **Rótulo da Rede**.  
Especifique o mesmo rótulo que o especificado para a rede da máquina virtual *vSwitch1*.  
Por exemplo: *VMkernel iSCSI*.
  4. Ligue o adaptador iSCSI recém-criado ao **VMkernel Network Adapter**.  
Siga as instruções no procedimento “Ligar adaptadores iSCSI a adaptadores VMkernel” do VMware. No momento desta publicação, o procedimento a seguir estava disponível em VMware ESXi and vCenter Server 5 Documentation.
- Tip:** Se ocorrer um tempo limite quando dispositivos iSCSI forem varridos, reduza o número de dispositivos iSCSI conectados ao host ESXi. Em seguida, varra os dispositivos iSCSI novamente.
5. Verifique se as propriedades de ligação do adaptador iSCSI estão corretas.
    - a. Acesse **Hardware > Adaptadores de Armazenamento** no VMware vSphere Client.
    - b. Clique com o botão direito no adaptador iSCSI e selecione **Propriedades do inicializador do iSCSI**. Certifique-se de que as propriedades de ligação a seguir existam:

Tabela 15. Configurações de rede do iSCSI

Rede de Máquina Virtual	Rede iSCSI
<b>Comutador Padrão:</b> <i>vSwitch0</i>	<b>Comutador Padrão:</b> <i>vSwitch1</i>
<b>Grupo da Porta da Máquina Virtual:</b> <i>MV Network</i>	<b>Porta VMkernel:</b> <i>VMkernel iSCSI</i> <b>Tip:</b> <i>VMkernel iSCSI</i> é ligado ao <b>VMkernel Adapter:</b> <i>vmk1</i> , que está no <b>Adaptador de Rede Física:</b> <i>vmnic1</i> .
<b>Adaptador Físico:</b> <i>vmnic0</i>	<b>VMkernel Network Adapter:</b> <i>vmk1</i>
	<b>Adaptador de Rede Física:</b> <i>vmnic1</i>
	<b>Endereço IP</b> do Adaptador de Rede Virtual: 192.168.42.x (sub-rede para a rede iSCSI)



## Results

Uma rede iSCSI dedicada está pronta para as operações de acesso instantâneo e restauração instantânea da MV completa.

---

## Configurando a comunicação com Segurança da Camada de Transporte

O GUI do Data Protection for VMware vSphere usa o protocolo de Segurança da Camada de Transporte (TLS) para se comunicar com seu cliente de GUI da web e com o servidor IBM Spectrum Protect.

### Sobre Esta Tarefa

O GUI do Data Protection for VMware vSphere sempre usa o protocolo HTTPS para se comunicar com navegadores da web. Em outras palavras, a TLS está sempre ativada. Durante a instalação do Proteção de Dados para VMware, é gerado um certificado digital autoassinado que, em seguida, é usado para as sessões do navegador da web.

Se quiser utilizar um certificado que seja assinado por um terceiro (conhecido como autoridade de certificação), siga as etapas descritas em “Usando um certificado de terceiros”.

A comunicação de TLS com o servidor IBM Spectrum Protect é opcional e não é ativada por padrão. Para ativá-la, siga as etapas descritas em “Ativando a comunicação segura com o servidor IBM Spectrum Protect” na página 60.

## Usando um certificado de terceiros

Para usar um certificado que seja assinado por um terceiro (conhecido como autoridade de certificação), deve-se concluir várias etapas.

### Sobre Esta Tarefa

Os procedimentos a seguir usam a ferramenta de gerenciamento de certificado e chave padrão chamada **keytool**.

Em sistemas operacionais Linux, elas estão localizadas no diretório `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Em sistemas operacionais Microsoft Windows, elas estão localizadas no diretório `C:\IBM\tivoli\tsm\tdpvmware\webserver\jre\jre\bin`.

Talvez seja necessário especificar o caminho completo durante a execução de **keytool** na linha de comandos.

### Procedimento

1. Obtenha acesso ao keystore.
2. Crie um Certificate Signing Request (CSR).
3. Envie o Certificate Signing Request para a autoridade de certificação assinar.
4. Receba o certificado assinado no GUI do Data Protection for VMware vSphere.

## Obtendo acesso ao keystore

Certificados são armazenados em um Java™ keystore. O conteúdo do keystore é protegido por senha. Para manipular os certificados no keystore, deve-se obter acesso ao keystore.

## Sobre Esta Tarefa

O certificado autoassinado padrão e a senha do keystore são gerados automaticamente durante a instalação, portanto, é improvável que você saiba a senha inicial.

Conclua o procedimento a seguir para substituir o keystore original por um novo keystore e um novo certificado autoassinado. O novo keystore é protegido por uma senha de sua escolha.

Se você já souber a senha do keystore, ignore esse procedimento.

## Procedimento

1. Pare o serviço GUI do Data Protection for VMware vSphere.
2. A partir da linha de comandos, mude o diretório para o local do keystore.
  - No Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
  - No Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\resources\security\`
3. Faça uma cópia de backup do arquivo keystore (`key.jks`) renomeando-o ou movendo-o para um local diferente.
4. Crie um novo keystore e um novo certificado autoassinado emitindo o seguinte comando:

```
keytool -genkeypair -alias vekey -dname
CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM
-keyalg RSA
-sigalg SHA256withRSA -keysize 2048 -validity days
-keystore
key.jks -storepass password -keypass
password
```

Em que:

**-dname CN=fqdn,OU=Tivoli\_Storage\_Manager\_for\_VMware,O=IBM**

*fqdn* é o nome do DNS ou nome completo do domínio do computador no qual o GUI do Data Protection for VMware vSphere está instalado.

**-validitydays**

O período de validade do certificado.

**-storepass password**

A senha do armazenamento de chaves. Assegure-se de se lembrar dessa senha para uso futuro.

**-keypass password**

A senha de chave privada para o certificado. Essa senha deve corresponder à senha do keystore.

5. Codifique a senha do keystore usando a ferramenta **securityUtility**. Emita o seguinte comando.
  - No Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`

- No Windows: C:\IBM\tivoli\tsm\tdpvmware\webserver\bin\securityUtility.bat encode

Insira a senha do keystore quando solicitado e salve a saída (por exemplo, copie-a na área de transferência).

6. Abra o arquivo `bootstrap.properties` em um editor e configure a propriedade `veProfile.keystore.pswd` para o valor codificado da etapa anterior. O arquivo `bootstrap.properties` está no seguinte local:

- No Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`
- No Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\`

7. Inicie o serviço do GUI do Data Protection for VMware vSphere.

#### Referências relacionadas:

“Iniciando e Executando Serviços para Proteção de Dados para VMware” na página 80

## Criando um Certificate Signing Request

Após ter obtido acesso ao keystore, deve-se criar um Certificate Signing Request (CSR).

### Procedimento

Conclua as etapas a seguir para criar um CSR:

1. A partir da linha de comandos, mude o diretório para o local do keystore.

- No Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
- No Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\resources\security\`

2. Crie um novo certificado emitindo o comando a seguir:

```
keytool -genkeypair -alias mykey -dname
CN=fqdn,OU=unit,O=organization
-keyalg RSA -sigalg SHA256withRSA
-keysize 2048 -validity days -keystore key.jks
-storepass
password -keypass password
```

Em que:

**-alias mykey**

*mykey* é o alias exclusivo que identifica o certificado no keystore. Ele é renomeado quando o certificado assinado é recebido.

**-dname CN=fqdn,OU=unit,O=organization**

*fqdn* é o nome do DNS ou nome completo do domínio do computador no qual o GUI do Data Protection for VMware vSphere está instalado.

*Unit* e *organization* são as informações da organização requeridas por suas políticas ou pela autoridade de certificação.

**-validitydays**

O período de validade do certificado.

**-storepass password**

A senha do armazenamento de chaves. Se não souber ou se esquecer a senha do keystore, consulte “Obtendo acesso ao keystore” na página 56.

**-keypass** *password*

A senha de chave privada para o certificado. Essa senha deve corresponder à senha do keystore.

3. Crie um CSR emitindo o comando a seguir:

```
keytool -certreq -alias mykey -file  
certreq.pem -keystore key.jks
```

Em que:

**-alias** *mykey*

O alias de certificado da etapa anterior.

**-file** *certreq.pem*

O arquivo para armazenar o Certificate Signing Request.

## Enviando o Certificate Signing Request para a autoridade de certificação

Após criar a solicitação de certificado (*certreq.pem*), deve-se enviá-la para a autoridade de certificação para assinatura. Siga as instruções específicas da autoridade de certificação.

## Recebendo o certificado assinado

Após obter o certificado assinado da autoridade de certificação (CA), deve-se receber o certificado no keystore.

## Procedimento

Para receber o certificado assinado, conclua as etapas a seguir:

1. A partir da linha de comandos, mude o diretório para o local do keystore.
  - No Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
  - No Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\resources\security\`
2. Copie os arquivos que você recebeu da autoridade de certificação (CA) nesse local. Esses arquivos incluem o certificado raiz da CA, certificados de CA intermediários (se houver) e o certificado assinado para GUI do Data Protection for VMware vSphere.
3. Pare o serviço GUI do Data Protection for VMware vSphere.
4. Faça uma cópia de backup do arquivo keystore (*key.jks*) copiando-o em um nome ou local diferente.
5. Importe os certificados de CA intermediários, se houver, com o comando a seguir. Quando for perguntado sobre a confiança nos certificados, responda *yes*. Repita essa etapa para várias CAs intermediárias conforme necessário.

```
keytool -importcert -alias  
ca-intermediate -file  
intermediate.pem  
-keystore key.jks -storepass password
```

Em que:

**-alias** *ca-intermediate*

O alias exclusivo que identifica o certificado no keystore. Cada certificado intermediário deve ter um alias exclusivo.

**-file** *intermediate.pem*

O arquivo de certificado intermediário que é obtido da CA.

**-storepass** *password*

A senha do keystore.

6. Importe o certificado raiz da CA emitindo o seguinte comando. Quando for perguntado sobre a confiança nesse certificado, responda *yes*.

```
keytool -importcert -alias ca-root  
-file root.pem -keystore  
key.jks -storepass password
```

Em que:

**-alias** *ca-root*

O alias exclusivo que identifica o certificado no keystore.

**-file** *root.pem*

O arquivo de certificado raiz obtido da CA.

**-storepass** *password*

A senha do keystore.

7. Importe o certificado assinado emitindo o seguinte comando:

```
keytool -importcert -alias mykey -file  
signedcert.pem -keystore  
key.jks -storepass password
```

Em que:

**-alias** *mykey*

O alias para o certificado assinado. O alias deve ser o mesmo que o usado durante a geração do Certificate Signing Request (CSR).

**-file** *signedcert.pem*

O arquivo de certificado assinado recebido da CA.

**-storepass** *password*

A senha do keystore.

8. Exclua o certificado existente que contém o alias *vekey*:

```
keytool -delete -alias vekey -keystore key.jks -storepass  
password
```

Em que **-storepass** *password* é a senha para o keystore.

9. Renomeie o certificado assinado para *vekey*:

```
keytool -changealias -alias mykey  
-destalias vekey -keystore  
key.jks -storepass password
```

Em que:

**-alias** *mykey*

O alias do certificado assinado.

**-storepass** *password*

A senha do keystore.

10. Inicie o serviço do GUI do Data Protection for VMware vSphere.

#### Referências relacionadas:

“Iniciando e Executando Serviços para Proteção de Dados para VMware” na página 80

## Ativando a comunicação segura com o servidor IBM Spectrum Protect

Se o servidor IBM Spectrum Protect estiver configurado para usar o protocolo Secure Sockets Layer (SSL) ou Segurança da Camada de Transporte (TLS), é possível ativar o GUI do Data Protection for VMware vSphere para se comunicar com o servidor pelo protocolo SSL ou TLS.

### Antes de Iniciar

Se o servidor estiver usando um certificado autoassinado, deve-se obter uma cópia desse certificado do administrador do servidor.

Se o servidor estiver usando um certificado de terceiros, deve-se obter o certificado raiz da autoridade de certificação (CA).

### Sobre Esta Tarefa

O procedimento a seguir usa ferramenta de gerenciamento de certificado e chave Java, **keytool**.

Em sistemas operacionais Linux, a ferramenta está no diretório `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

Em sistemas operacionais Microsoft Windows, a ferramenta está no diretório `C:\IBM\tivoli\tsm\tdpvmware\webserver\jre\jre\bin\`.

Talvez seja necessário especificar o caminho completo quando você executar o comando **keytool**.

### Procedimento

1. A partir da linha de comandos, mude o diretório para o local do armazenamento confiável:
  - No Linux: `/opt/tivoli/tsm/tdpvmware/common/scripts/`
  - No Windows: `C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts\`
2. Crie o armazenamento confiável e importe o certificado com o comando a seguir:

```
keytool -importcert -alias my-cert  
-file cert.pem -keystore  
tsm-ve-truststore.jks -storepass password
```

Em que:

**-alias** *my-cert*

O alias exclusivo que identifica o certificado no armazenamento confiável.

**-file** *cert.pem*

O arquivo que contém o certificado autoassinado do servidor ou o certificado raiz da CA.

**-storepass** *password*

A senha do armazenamento de chaves. Assegure-se de se lembrar dessa senha para uso futuro.

3. Inicie o GUI do Data Protection for VMware vSphere e acesse a janela Configuração.

- Se você estiver criando uma configuração inicial, clique em **Executar Assistente de Configuração** e acesse a página Credenciais do Servidor.
  - Se você estiver modificando uma configuração existente, clique em **Editar Configuração** e vá para a página Credenciais do Servidor.
4. Insira o número da porta no campo **Porta do Administrador do IBM Spectrum Protect**.  
O número da porta a ser usado normalmente é o valor especificado pela opção SSLTCPPort no arquivo de opções do servidor (dsmserv.opt). Entretanto, se a instrução ADMINONCLIENT NO for especificada no arquivo dsmserv.opt, o número da porta correto a ser usado para o protocolo SSL será o valor especificado pela opção SSLTCPADMINPort.
  5. Selecione **Usar Comunicações SSL na Porta do Administrador**.
  6. Se desejar usar essa configuração para futuras sessões da GUI, selecione **Salvar a configuração de ID, senha e porta de administrador**.
  7. Clique em **OK** para aplicar as alterações.

---

## Requisitos de privilégio de usuário do VMware vCenter Server

Certos privilégios do VMware vCenter Server são necessários para executar operações do Proteção de Dados para VMware.

### Privilégios do vCenter Server necessários para proteger datacenters do VMware com a visualização do navegador da web para o GUI do Data Protection for VMware vSphere

O ID do usuário do vCenter Server que efetua sign on na visualização do navegador para o GUI do Data Protection for VMware vSphere

deve ter privilégios suficientes do VMware para visualizar o conteúdo de um datacenter gerenciado pela GUI.

Por exemplo, um ambiente VMware vSphere contém cinco datacenters. Um usuário, "jenn", tem privilégios suficientes para somente dois desses datacenters. Como resultado, somente esses dois datacenters, nos quais existem privilégios suficientes, são visíveis para "jenn" nas visualizações. Os outros três datacenters (para os quais "jenn" não tem privilégios) não estarão visíveis para o usuário "jenn".

O VMware vCenter Server define um conjunto de privilégios coletivamente como uma função. Uma função é aplicada a um objeto para um usuário ou grupo especificado para criar um privilégio. No VMware vSphere Web Client, você deve criar uma função com um conjunto de privilégios. Para criar uma função do vCenter Server para as operações de backup e restauração, use a função **Incluir uma Função** do VMware vSphere Client. Você deve designar esta função a um ID do usuário para um vCenter Server ou datacenter especificado. Se desejar propagar os privilégios para todos os datacenters dentro do vCenter, especifique o vCenter Server e marque a caixa de seleção propagar para filhos. Caso contrário, é possível limitar as permissões se designar a função para os datacenters necessários apenas com a caixa de seleção propagar para os filhos selecionada. A execução da GUI do navegador é no nível do datacenter.

O seguinte exemplo mostra como controlar o acesso aos datacenters para dois grupos de usuário do VMware. Primeiro, crie uma função que contenha todos os privilégios definidos na nota técnica 7047438. O conjunto de privilégios neste

exemplo é identificado pela função chamada “TDPVMwareManage”. O Grupo 1 requer acesso para gerenciar máquinas virtuais para os datacenters Primary1\_DC e Primary2\_DC. O Grupo 2 requer acesso para gerenciar máquinas virtuais para os datacenters Secondary1\_DC e Secondary2\_DC.

Para o Grupo 1, designe a função “TDPVMwareManage” para os datacenters Primary1\_DC e Primary2\_DC. Para o Grupo 2, designe a função “TDPVMwareManage” para os datacenters Secondary1\_DC e Secondary2\_DC.

Os usuários em cada grupo de usuários do VMware podem usar a GUI do Proteção de Dados para VMware para gerenciar máquinas virtuais apenas em seus respectivos datacenters.

**Dica:** Ao criar uma função, considere incluir privilégios extras na função que você pode precisar posteriormente para concluir outras tarefas em objetos.

### **Privilégios do vCenter Server necessários para usar o movedor de dados**

O movedor de dados do IBM Spectrum Protect instalado no servidor de backup vStorage (o nó do movedor de dados) requer as opções VMCUser e VMCPw. A opção VMCUser especifica o ID do usuário do servidor vCenter ou ESX que deseja fazer backup, restaurar ou consultar. Os privilégios necessários que são designados ao ID do usuário (VMCUser) asseguram que o cliente possa executar operações na máquina virtual e no ambiente VMware. Este ID do usuário deve ter os privilégios do VMware que são descritos em nota técnica 7047438.

Para criar uma função do vCenter Server para as operações de backup e restauração, use a função **Incluir uma Função** do VMware vSphere Client. Deve-se selecionar a opção propagar para os filhos ao incluir privilégios para esse ID do usuário (VMCUser). Além disso, considere incluir outros privilégios a essa função para tarefas diferentes de backup e restauração. Para a opção VMCUser, a execução está no objeto de nível superior.

### **Privilégios do vCenter Server necessários para proteger datacenters do VMware com a visualização do Extensão do IBM Spectrum Protect para o GUI do Data Protection for VMware vSphere**

O Extensão do IBM Spectrum Protect requer um conjunto de privilégios que são separados dos privilégios necessários para efetuar sign on na GUI.

Durante a instalação, os seguintes privilégios customizados são criados para o Extensão do IBM Spectrum Protect:

- **Datacenter > IBM Data Protection**
- **Global > IBM Data Protection**

Os privilégios customizados requeridos para o Extensão do IBM Spectrum Protect são registrados como uma extensão separada. A chave de extensão de privilégios é `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Esses privilégios permitem que o administrador do VMware ative e desative o acesso ao conteúdo do Extensão do IBM Spectrum Protect. Apenas os usuários com esses privilégios customizados no objeto do VMware requerido podem acessar o conteúdo do Extensão do IBM Spectrum Protect. Um Extensão do IBM Spectrum



Protect é registrado para cada vCenter Server e é compartilhado por todos os hosts da GUI que são configurados para suportar o vCenter Server.

No Web client do VMware vSphere, deve-se criar uma função para os usuários que podem executar funções de proteção de dados para máquinas virtuais, utilizando o Extensão do IBM Spectrum Protect. Para essa função, além dos privilégios da função de administrador da máquina virtual padrão requeridos pelo web client, você deve especificar o privilégio **Datacenter > IBM Data Protection**. Para cada datacenter, designe esta função para cada usuário ou grupo de usuários em que deseja conceder permissão para o usuário gerenciar máquinas virtuais.

O privilégio **Global > IBM Data Protection** é necessário para o usuário no nível do vCenter. Esse privilégio permite que o usuário gerencie, edite ou limpe a conexão entre o vCenter Server e o servidor da web do GUI do Data Protection for VMware vSphere. Designe esse privilégio para os administradores que estão familiarizados com o GUI do Data Protection for VMware vSphere que protege seus respectivos vCenter Servers. Gerencie suas conexões do Extensão do IBM Spectrum Protect na página Conexões da extensão.

O seguinte exemplo mostra como controlar o acesso aos datacenters para dois grupos de usuário. O grupo 1 requer acesso para gerenciar máquinas virtuais para os datacenters NewYork\_DC e Boston\_DC. O grupo 2 requer acesso para gerenciar máquinas virtuais para os datacenters LosAngeles\_DC e SanFrancisco\_DC.

No cliente VMware vSphere, crie, por exemplo, a função “IBMDDataProtectManage”, designe os privilégios de função de administrador da máquina virtual padrão e também o privilégio do **Datacenter > IBM Data Protection**.

Para o Grupo 1, designe a função “IBMDDataProtectManage” para os datacenters NewYork\_DC e Boston\_DC. Para o Grupo 2, designe a função “IBMDDataProtectManage” para os datacenters LosAngeles\_DC e SanFrancisco\_DC.

Os usuários em cada grupo podem usar o Extensão do IBM Spectrum Protect no Web client do vSphere para gerenciar máquinas virtuais apenas em seus respectivos datacenters.

## Problemas relacionados a permissões insuficientes

Quando o usuário do navegador da web não tem permissões suficientes para nenhum datacenter, o acesso à visualização é bloqueado. Em vez disso, a mensagem de erro GVM2013E é emitida para avisar que o usuário não está autorizado a acessar nenhum datacenter gerenciado devido a permissões insuficientes. Estão disponíveis também outras mensagens novas que informam aos usuários sobre os problemas que resultam de permissões insuficientes. Para resolver quaisquer problemas relacionados a permissões, assegure-se de que a função de usuário esteja configurada conforme descrito nas seções anteriores. A função de usuário deve ter todos os privilégios identificados na tabela de IDs de usuários e movedores de dados de privilégios requeridos do vCenter Server e esses privilégios devem ser aplicados no nível do datacenter com a caixa de seleção propagar para filhos.

Quando o usuário do Extensão do IBM Spectrum Protect não tem permissões suficientes para um datacenter, as funções de proteção de dados para esse datacenter e seu conteúdo ficam indisponíveis na extensão.

Quando o ID do usuário IBM Spectrum Protect (especificado pela opção VMCUser) contém permissões insuficientes para as operações de backup ou restauração, a seguinte mensagem é exibida:

```
ANS9365E Erro de API do VMware vStorage.  
"A permissão para executar essa operação foi negada."
```

Quando o ID do usuário do IBM Spectrum Protect contém permissões insuficientes para visualizar uma máquina, as mensagens a seguir são mostradas:

```
Comando de backup da VM iniciado. Número total de máquinas virtuais a processar: 1  
ANS4155E A Máquina Virtual 'tango' não pôde ser localizada no servidor VMware.  
ANS4148E Um backup completo da Máquina Virtual 'foxtrot' falhou com o RC 4390
```

Para recuperar as informações de log por meio do VMware Virtual Center Server sobre problemas de permissão, conclua essas etapas:

1. Em Configurações do vCenter Server, selecione **Opções de criação de log** e configure **"Criação de log do vCenter como Trivia (Trivia)**.
2. Recrie o erro de permissão.
3. Reconfigure **Criação de log do vCenter** para seu valor anterior para evitar registrar informações de log em excesso.
4. Em Logs do sistema, procure o log mais atual do vCenter Server (vpxd-wxyz.log) e procure a sequência NoPermission. Por exemplo:  

```
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:  
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE  
Throw: vim.fault.NoPermission
```

Essa mensagem de log indica que o ID do usuário não continha permissões suficientes para criar uma captura instantânea (createSnapshot).

---

## Funções de Usuário do GUI do Data Protection for VMware vSphere

A disponibilidade das funções do GUI do Data Protection for VMware vSphere se baseia no nível de autoridade designado ao ID de administrador do IBM Spectrum Protect.

O ID de administrador deve corresponder ao nome do nó. Em liberações anteriores do produto, o comando **REGISTER NODE** criava automaticamente um ID de usuário administrativo cujo nome correspondia ao nome do nó. A partir da IBM Spectrum Protect V8.1, o comando **REGISTER NODE** não cria automaticamente um ID de usuário administrativo que corresponde ao nome do nó.

Ao registrar um novo nó, o administrador do servidor IBM Spectrum Protect deve especificar o parâmetro `userid` com o comando do servidor **REGISTER NODE**:

```
REGISTER NODE node_name password userid=user_id
```

Em que o nome do nó e o ID do usuário administrativo devem ser iguais. Por exemplo:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

Por padrão, o nó tem autoridade do proprietário cliente.

As tarefas que podem ser executadas com o GUI do Data Protection for VMware vSphere baseiam-se na classe de privilégio designada ao ID de administrador.

Quando o ID de administrador não tiver privilégios de domínio de política irrestritos, não será possível registrar novos nós ou configurar seu relacionamento

de proxy no servidor IBM Spectrum Protect. Se você não inserir um ID de administrador, um script da macro será criado para que seja possível executar no servidor IBM Spectrum Protect.

Um ID de administrador do IBM Spectrum Protect é solicitado ao configurar o GUI do Data Protection for VMware vSphere. Esta tabela lista as funções que estão disponíveis com base na classe de privilégios designada a esse ID:

- Um valor Sim indica função disponível para a função de usuário.
- Um valor Não indica função não disponível para a função de usuário.

Para visualizar sua função do GUI do Data Protection for VMware vSphere atual, passe o mouse sobre o ID do usuário na barra de navegação.

*Tabela 16. Funções disponíveis baseadas nos requisitos de privilégio de ID do administrador do IBM Spectrum Protect*

	Operador	Operador com Relatório	Administrador Restrito	Administrador
<b>Resumo</b>	Executar agora backup e restauração	Operador mais relatório	Operador mais operações de relatório e planejamento para domínios de políticas listados	Todas as funções, incluindo configuração inicial
<b>ID de Administrador do IBM Spectrum Protect Classe de Privilégio</b>	Nenhuma	Uma das seguintes classes de privilégio: <ul style="list-style-type: none"> <li>• Armazenamento</li> <li>• Operador</li> <li>• Analista</li> </ul>	Política (Restrita) ou uma das seguintes classes de privilégio: <ul style="list-style-type: none"> <li>• Armazenamento</li> <li>• Operador</li> <li>• Analista</li> </ul>	Política (Irrestrita) ou Sistema

#### Guia Backup

Gerenciar tarefas de backup <b>Executar agora</b>	Sim	Sim	Sim	Sim
Gerenciar tarefas de backup <b>Planejadas</b>	Não <sup>1</sup>	Não <sup>1</sup>	Sim, dentro dos domínios de política	Sim
Visualizar tarefas de backup <b>Executar agora</b>	Sim	Sim	Sim	Sim
Visualizar tarefas de backup <b>Planejadas</b>	Não	Sim	Sim	Sim
Excluir uma tarefa de backup <b>Planejada</b>	Não	Não	Sim, nos domínio de política	Sim

Tabela 16. Funções disponíveis baseadas nos requisitos de privilégio de ID do administrador do IBM Spectrum Protect (continuação)

	Operador	Operador com Relatório	Administrador Restrito	Administrador
<b>Guia Restaurar</b>				
Executar uma tarefa de <b>Restauração</b>	Sim	Sim	Sim	Sim
<b>Guia Relatórios</b>				
Eventos	Não	Sim	Sim	Sim
Tarefas Recentes	Sim	Sim	Sim	Sim
Status do Backup	Não	Sim	Sim	Sim
Proteção do Aplicativo	Não	Sim	Sim	Sim
Ocupação do Datacenter	Não	Sim	Sim	Sim
<b>Guia Configuração</b>				
Registro do Nó (Status da Configuração -> <b>Assistente para Executar Configuração</b> )	Não	Não	Não <sup>2</sup>	Sim
Mudar credenciais do ID de administrador do IBM Spectrum Protect (Status da Configuração -> <b>Editar Configuração</b> )	Sim	Sim	Sim	Sim
Mudar Senha do nó VMCLI (Status da Configuração -> <b>Editar Configuração</b> )	Não	Não	Sim	Sim
Mudar domínios de GUI (Status da configuração -> <b>Configuração de edição</b> )	Sim <sup>3</sup>	Sim <sup>3</sup>	Sim <sup>3</sup>	Sim

Tabela 16. Funções disponíveis baseadas nos requisitos de privilégio de ID do administrador do IBM Spectrum Protect (continuação)

	Operador	Operador com Relatório	Administrador Restrito	Administrador
Mudar nós do movedor de dados (Status da configuração -> <b>Configuração de edição</b> )	Não	Não	Não <sup>2</sup>	Sim
Mudar nós do proxy de montagem (Status da Configuração -> <b>Editar Configuração</b> )	Não	Não	Não <sup>2</sup>	Sim

1. Não é possível registrar o nó porque uma política de domínio irrestrita é necessária.
2. É possível incluir ou remover os datacenters do VMware e registrar os nós do datacenter.

Para visualizar o nível de autoridade do ID de administrador do IBM Spectrum Protect e a função do GUI do Data Protection for VMware vSphere correspondente:

1. Acesse a janela Configuração.
2. Clique em **Editar Configuração**.
3. As informações relevantes são mostradas na página Credenciais do Spectrum Protect Server.

#### Importante:

- Se o nível de autoridade do ID de administrador do IBM Spectrum Protect for alterado no servidor IBM Spectrum Protect, o GUI do Data Protection for VMware vSphere deverá ser reiniciado para refletir essa mudança.
- Ao alterar a Função de Usuário, você deve clicar em **OK** para salvar suas mudanças antes de acessar outra página Definições de Configuração ou tentar outra mudança na configuração. Caso contrário, as mudanças na Função de Usuário não entrarão em vigor.

## Chaves de registro da GUI do Proteção de Dados para VMware

Dependendo das opções selecionadas durante a instalação, é possível acessar a GUI do Proteção de Dados para VMware usando métodos diferentes. Chaves de registro são criadas para as GUIs do Proteção de Dados para VMware.

A frase “GUI do Proteção de Dados para VMware” se aplica às GUIs a seguir:

- GUI do Data Protection for VMware vSphere acessada em um navegador da web
- Extensão do IBM Spectrum Protect na GUI do vSphere Web Client

A chave de registro do Extensão do IBM Spectrum Protect é `com.ibm.tsm.tdpvmware.IBMDataProtection`. Essa chave é registrada ao selecionar a

caixa de opções **Registrar a extensão do vSphere Web Client** durante a instalação. Uma única instância do Extensão do IBM Spectrum Protect é registrada por servidor vCenter.

Uma chave de registro não é criada para o GUI do Data Protection for VMware vSphere que é acessado em um navegador da web.

Para visualizar as chaves de registro, efetue login no VMware Managed Object Browser (MOB). Após efetuar login no MOB, acesse **Conteúdo>Gerenciador de Extensões** para visualizar as chaves de registro.

---

## Configurando a GUI do agente de recuperação

Instruções sobre como configurar a GUI do agente de recuperação para operações de montagem, restauração de arquivo ou restauração instantânea são fornecidas.

### Antes de Iniciar

Estas tarefas de configuração devem ser concluídas antes de você tentar uma operação na GUI do agente de recuperação.

**Importante:** Informações sobre como concluir tarefas com a GUI do agente de recuperação são fornecidas na ajuda on-line instalada com a GUI. Clique em **Ajuda** em qualquer uma das janelas da GUI para abrir a ajuda online e obter assistência de tarefa.

### Procedimento

1. Efetue logon no sistema em que deseja restaurar arquivos. O agente de recuperação deve estar instalado no sistema.
2. Clique em **Selecionar servidor TSM** na GUI do agente de recuperação para se conectar a um servidor IBM Spectrum Protect. Quando o agente de recuperação é instalado no mesmo sistema que o GUI do Data Protection for VMware vSphere e os aplicativos foram configurados com êxito usando o assistente de configuração do GUI do Data Protection for VMware vSphere, existirão as seguintes condições:
  - O nó do movedor de dados e o servidor IBM Spectrum Protect são preenchidos no campo agente de recuperação Servidor TSM.
  - Os campos a seguir são preenchidos no painel Informações do Servidor TSM:
    - O **Nó de autenticação** contém uma lista de nós do movedor de dados disponíveis.
    - O **Nó de destino** contém uma lista de nós do datacenter que estão disponíveis para o nó do movedor de dados selecionado.

Quando somente um nó do movedor de dados tiver sido definido localmente com o assistente de configuração, o agente de recuperação usa esse nó para autenticação quando iniciado. O agente de recuperação lembra o último nome do nó conectado ao servidor IBM Spectrum Protect. Se **Usar Senha para Gerar Acesso** for selecionada para esse nó (o último nome do nó conectado), o agente de recuperação usará estas credenciais para conectar-se ao servidor IBM Spectrum Protect na inicialização. Se nenhuma conexão anterior com o servidor IBM Spectrum Protect foi estabelecida e apenas um nó do movedor de dados e um nó do datacenter forem configurados com o assistente, o agente de recuperação usará essas credenciais para conectar-se ao servidor IBM Spectrum Protect na inicialização.

Especifique as seguintes opções:

### Endereço do Servidor

Insira o endereço IP ou nome do host do IBM Spectrum Protect.

### Porta do Servidor

Insira o número da porta usado para comunicação TCP/IP com o servidor. O número da porta padrão é 1500.

Método de acesso do nó:

### Asnodename

Selecione essa opção para usar um nó de proxy para acessar backups de MV que estão no nó de destino. O nó de proxy é um nó ao qual é concedida a autoridade de "proxy" para executar operações em nome do nó de destino.

Normalmente, o administrador do IBM Spectrum Protect usa o comando `grant proxynode` para criar o relacionamento de proxy entre dois nós existentes.

Se você selecionar essa opção, conclua as etapas a seguir:

- Insira o nome do nó de destino (o nó em que os backups de MV estão localizados) no campo **Nó de Destino**.
- Insira o nome do nó de proxy no campo **Nó de Autenticação**.
- Insira a senha para o nó de proxy no campo **Senha**.
- Clique em **OK** para salvar essas configurações e sair do diálogo de informações do IBM Spectrum Protect.

Quando você usa esse método, o usuário do agente de recuperação conhece apenas a senha do nó do proxy e a senha do nó de destino está protegida.

### Fromnode

Selecione essa opção para usar um nó com acesso limitado apenas aos dados de captura instantânea de VMs específicas no nó de destino.

Normalmente, a esse nó é dado acesso do nó de destino que possui os backups da MV usando o comando `set access`:

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

Por exemplo, esse comando concede ao nó denominado `myMountNode` a autoridade para restaurar arquivos da MV denominada `myTestVM`:

```
set access backup -TYPE=VM myTestVM myMountNode
```

Se você selecionar essa opção, conclua as etapas a seguir:

- Insira o nome do nó de destino (o nó em que os backups de MV estão localizados) no campo **Nó de Destino**.
- Insira o nome do nó ao qual é concedido acesso limitado no campo **Nó de Autenticação**.
- Insira a senha do nó ao qual é concedido acesso limitado no campo **Senha**.
- Clique em **OK** para salvar essas configurações e sair do diálogo de informações do IBM Spectrum Protect.

Ao usar esse método, é possível ver uma lista completa de VMs com backup. Entretanto, só é possível restaurar aqueles backups de VMs aos quais o nó tem acesso. Além disso, os dados de captura instantânea não estão protegidos contra expiração no servidor. Como resultado, a restauração instantânea não é suportada nesse método.

### Direcionar

Selecione essa opção para autenticar diretamente no nó de destino (o nó em que os backups de VMs estão localizados).

Se você selecionar essa opção, conclua as etapas a seguir:

- a. Insira o nome do nó de destino (o nó em que os backups de VMs estão localizados) no campo **Nó de Autenticação**.
- b. Insira a senha para o nó de destino no campo **Senha**.
- c. Clique em **OK** para salvar essas configurações e sair do diálogo de informações do IBM Spectrum Protect.

### Usar Senha para Gerar Acesso

Quando essa opção está selecionada e o campo de senha está vazio, o agente de recuperação é autenticado com uma senha existente armazenada no registro. Se não estiver selecionada, você deverá inserir a senha manualmente.

Para usar essa opção, você deve primeiramente configurar manualmente uma senha inicial para o nó ao qual a opção se aplica. Você deve especificar a senha inicial ao se conectar ao nó do IBM Spectrum Protect pela primeira vez, inserindo a senha no campo **Senha** e selecionando a caixa de opção **Usar senha para gerar acesso**.

No entanto, ao usar o nó do movedor de dados local como o **Nó de Autenticação**, a senha pode já estar armazenada no registro. Como resultado, selecione a caixa de opção **Usar senha para gerar acesso** e não insira uma senha.

O agente de recuperação consulta o servidor especificado para obter uma lista de MVs protegidas e mostra a lista.

3. Configure as seguintes opções de montagem, backup e restauração clicando em **Configurações**:

### Cache de gravação de Volume Virtual

O agente de recuperação que está em execução no host do proxy de backup do Windows salva mudanças de dados que são criadas durante a restauração instantânea e montagem. Essas mudanças são salvas em um volume virtual no cache de gravação. Por padrão, o cache de gravação é ativado e especifica o caminho C:\ProgramData\Tivoli\TSM\TDPVMware\mount\ e o tamanho de cache máximo de 90% de espaço disponível para a pasta selecionada. Para evitar que o volume do sistema fique cheio, altere o cache de gravação para um caminho em um volume que não seja o volume do sistema.

### Pasta para arquivos temporários

Especifique o caminho em que as mudanças de dados são salvas. O cache de gravação deve estar em uma unidade local e não pode ser configurado para um caminho em uma pasta compartilhada. Se o cache de gravação estiver desativado ou cheio, a tentativa de iniciar uma sessão de restauração instantânea ou montagem falhará.

### Tamanho do cache

Especifique o tamanho do cache de gravação. O tamanho máximo permitido do cache é de 90% do espaço disponível para a pasta selecionada.



**Restrição:** Para evitar qualquer interrupção durante o processo de restauração, exclua o caminho do cache de gravação de todas as configurações de proteção de software antivírus.

#### **Acesso a Dados**

Especifique o tipo de dados a ser processado. Se você estiver usando um dispositivo off-line (como fita ou biblioteca de fita virtual), deverá especificar o tipo de dados aplicável.

#### **Tipo de armazenamento**

Especifique um dos seguintes dispositivos de armazenamento dos quais montar a captura instantânea:

##### **Disco/Arquivo**

A captura instantânea é montada a partir de um disco ou arquivo. Esse dispositivo é o padrão.

**Fita** A captura instantânea é montada a partir de um conjunto de armazenamento em fita. Quando essa opção é selecionada, não é possível montar diversas capturas instantâneas ou executar uma operação de restauração instantânea.

**VTL** A captura instantânea é montada por meio de uma biblioteca de fita virtual off-line. Não são suportadas sessões de montagem simultâneas na mesma biblioteca de fita virtual.

**Nota:** Quando o tipo de armazenamento for alterado, você deve reiniciar o serviço para que as mudanças entrem em vigor.

#### **Desativar a proteção de expiração**

Durante uma operação de montagem, a captura instantânea no servidor IBM Spectrum Protect é bloqueada para evitar que expire durante a operação. A expiração pode ocorrer porque outra captura instantânea é incluída na sequência de captura instantânea montada. Esse valor especifica se a proteção de expiração deve ser desativada durante a operação de montagem.

- Para proteger a captura instantânea da expiração, não selecione essa opção. A captura instantânea no servidor IBM Spectrum Protect é bloqueada e é protegida da expiração durante a operação de montagem.
- Para desativar a proteção de expiração, selecione esta opção. Por padrão, essa opção é selecionada. A captura instantânea no servidor IBM Spectrum Protect não é bloqueada e não é protegida da expiração durante a operação de montagem. Como resultado, a captura instantânea pode expirar durante a operação de montagem. Essa expiração pode produzir resultados inesperados e impactar negativamente o ponto de montagem. Por exemplo, o ponto de montagem pode se tornar inutilizável ou conter erros. No entanto, a expiração não afeta a cópia ativa atual. A cópia ativa não pode expirar durante a operação.

Quando a captura instantânea estiver em um servidor de replicação de destino, a captura instantânea não poderá ser bloqueada, porque está no modo somente leitura. Uma tentativa de bloqueio pelo servidor faz com que a operação

de montagem falhe. Para evitar a tentativa de bloqueio e impedir essa falha, desative a proteção de expiração selecionando esta opção.

#### **Tamanho da Leia Mais Adiante (em blocos de 16 KB)**

Especifique o número de blocos de dados extras recuperados do dispositivo de armazenamento depois que uma solicitação de leitura é enviada para um único bloco. Os valores padrão são os seguintes:

- Disco ou arquivo: 64
- Fita: 1024
- VTL: 64

O valor máximo para qualquer dispositivo é 1024.

#### **Tamanho do cache da Leitura Antecipada (em blocos)**

Especifique o tamanho do cache onde os blocos de dados extras são armazenados. Os valores padrão são os seguintes:

- Disco ou arquivo: 10000
- Fita: 75000
- VTL: 10000

Como cada captura instantânea possui seu próprio cache, certifique-se de que planejar quantas capturas instantâneas serão montadas ou restauradas simultaneamente. O tamanho do cache acumulativo não pode exceder 75000 blocos.

#### **Tempo limite do driver (segundos)**

Este valor especifica a quantia de tempo para processar solicitações de dados a partir do driver do sistema de arquivos. Se o processamento não for concluído a tempo, a solicitação será cancelada e um erro será retornado ao driver do sistema de arquivos. Considere o aumento desse valor ao perceber tempos limite. Por exemplo, tempos limite podem ocorrer quando a rede está lenta, o dispositivo de armazenamento está ocupado ou diversas sessões de montagem ou restauração instantânea estão sendo processadas. Os valores padrão são os seguintes:

- Disco ou arquivo: 60
- Fita: 180
- VTL: 60

Clique em **OK** para salvar suas mudanças e sair de **Configurações**.

4. Verifique se cada nó de servidor IBM Spectrum Protect (que foi especificado com as opções `Asnodename` e `Fromnode`) permite que backups sejam excluídos. O agente de recuperação cria objetos temporários não usados durante as operações. A opção do servidor `BACKDElete=Yes` permite que esses objetos sejam removidos de forma que eles não sejam acumulados no nó.
  - a. Efetue login no servidor IBM Spectrum Protect e inicie uma sessão administrativa de cliente no modo de linha de comandos:  
`dsmadm -id=admin -password=admin -dataonly=yes`
  - b. Insira este comando:  
`Query Node <nodename> Format=Detailed`

Certifique-se de que a saída do comando para cada nó inclua a seguinte instrução:

```
Backup Delete Allowed?: Yes
```

Se essa instrução não estiver incluída, atualize cada nó com este comando:  
UPDate Node <nodename> BACKDElete=Yes

Execute o comando Query Node novamente para cada nó para verificar se cada nó permite a exclusão de backups.

5. Quando você usa o Recover Agent em uma rede iSCSI e o Recovery Agent não usa um movedor de dados, acesse o C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf file e especifique a tag [IMOUNT] e o parâmetro **Target IP**:

```
[IMOUNT config]
Target IP=<IP address of the network card on the system
that exposes the iSCSI targets.>
```

Por exemplo:

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

Após incluir ou mudar o parâmetro Target IP, reinicie a GUI ou a CLI do Agente de Recuperação.

## Ativando a comunicação segura do agente de recuperação para o servidor IBM Spectrum Protect

Se o servidor IBM Spectrum Protect estiver configurado para usar o protocolo Secure Sockets Layer (SSL) ou Segurança da Camada de Transporte (TLS), será possível ativar o agente de recuperação para se comunicar com o servidor usando o protocolo.

### Antes de Iniciar

Considere os requisitos a seguir antes de iniciar a configuração para comunicação segura com o servidor:

- Cada servidor que está ativado para SSL deve ter um certificado exclusivo. O certificado pode ser um dos seguintes tipos:
  - Um certificado autoassinado pelo servidor.
  - Um certificado emitido por um certificado de autoridade de certificação (CA) terceirizada. O certificado de autoridade de certificação pode ser de uma empresa, como a Symantec ou a Thawte, ou um certificado interno mantido dentro de sua empresa.
- Por motivos de desempenho, use SSL ou TLS apenas para sessões em que a segurança é necessária. Considere incluir mais recursos do processador no sistema do servidor para gerenciar o aumento de requisitos.
- Para que um cliente se conecte a um servidor que esteja usando o TLS Versão 1.2, o algoritmo de assinatura do certificado deve ser o Secure Hash Algorithm 1 (SHA-1) ou posterior. Se você estiver usando um certificado autoassinado para

um servidor que está usando o TLS V1.2, deve-se usar o certificado cert256.arm. Seu administrador do IBM Spectrum Protect pode precisar mudar o certificado padrão no servidor.

- Para desativar protocolos de segurança que são menos seguros que o TLS 1.2, inclua a opção **SSLDISABLELEGACYt1s yes** no arquivo C:\windows\system32\fb.opt ou C:\Windows\SysWOW64\fb.opt. O TLS 1.2 ou posterior ajuda a evitar ataques de programas maliciosos.

## Ativando comunicação segura usando um certificado autoassinado do servidor IBM Spectrum Protect

Se o servidor IBM Spectrum Protect estiver usando um certificado autoassinado, deve-se obter uma cópia desse certificado do administrador do servidor e configurar o agente de recuperação para se comunicar com o servidor usando o protocolo TLS ou SSL.

### Sobre Esta Tarefa

Cada servidor gera seu próprio certificado. Os servidores versão 6.3 e posterior geram arquivos que são denominados cert256.arm se o servidor estiver usando o TLS 1.2 ou posterior ou cert.arm se o servidor estiver usando uma versão anterior do SSL ou TLS. As versões do servidor anteriores à V6.3 geram arquivos que são denominados cert.arm independentemente do protocolo. Você deverá escolher o certificado que estiver configurado no servidor.

O arquivo de certificado é armazenado na estação de trabalho do servidor no diretório de instância do servidor. Por exemplo, C:\IBM\tivoli\tsm\server\bin\cert256.arm. Se o arquivo de certificado não existir, o arquivo de certificado será criado ao reiniciar o servidor com essas opções configuradas.

### Procedimento

Para ativar a comunicação SSL ou TLS do agente de recuperação para o servidor usando um certificado autoassinado:

1. Anexe o caminho binário do GSKit e o caminho da biblioteca à variável de ambiente PATH no cliente. Por exemplo:  

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;  
C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```
2. Se você estiver configurando SSL ou TLS no cliente pela primeira vez, deve-se criar o banco de dados de chaves do cliente local dsmcert.kdb. A partir do diretório C:\Windows\SysWOW64, execute o comando **gsk8capicmd\_64** conforme mostrado no exemplo a seguir:

```
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
```

A senha fornecida é usada para criptografar o banco de dados de chaves. A senha é armazenada automaticamente criptografada no arquivo stash (dsmcert.sth). O arquivo stash é usado pelo cliente para recuperar a senha do banco de dados de chaves.

3. Obtenha o certificado autoassinado do servidor.
4. Importe o certificado para o banco de dados dsmcert.kdb. Deve-se importar o certificado de cada cliente para o dsmcert.kdb. A partir do diretório C:\Windows\SysWOW64, execute o comando **gsk8capicmd\_64** conforme mostrado no exemplo a seguir:

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server server_name self-signed key"  
-file path_to_certificate -format ascii -trust enable
```

Vários certificados do servidor podem ser incluídos no banco de dados dsmcert.kdb para que o cliente possa se conectar a diferentes servidores. Diferentes certificados devem ter diferentes etiquetas. Use nomes significativos para os rótulos.

**Importante:** Para uma recuperação de desastre do servidor, se o certificado tiver sido perdido, o servidor gera automaticamente um novo certificado. Cada cliente deve então importar o novo certificado.

5. Após o certificado do servidor ser incluído no banco de dados dsmcert.kdb, inclua a opção `ssl yes` no arquivo `C:\Windows\SysWOW64\fb.opt` e atualize o valor da opção `tcpport`.

**Importante:**

O servidor geralmente é configurado para conexões SSL e TLS em uma porta diferente das conexões não SSL e TLS. Não especifique um número da porta não SSL ou TLS para o valor de `tcpport`. Se o valor de `tcpport` estiver incorreto, o agente de recuperação não poderá se conectar ao servidor.

Não é possível se conectar a uma porta não SSL ou TLS com um agente de recuperação que está ativado para SSL ou TLS ou se conectar uma porta SSL ou TLS para um agente de recuperação que não está ativado para SSL ou TLS.

6. Configure as portas SSL ou TLS corretas nos arquivos de configuração do agente de recuperação a seguir:
  - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
  - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

## **Ativando a comunicação segura usando um certificado de empresa terceirizada**

Se o servidor IBM Spectrum Protect estiver usando uma autoridade de certificação (CA) terceirizada, deve-se obter o certificado raiz da CA.

### **Sobre Esta Tarefa**

Se o certificado tiver sido emitido por uma CA, como a Symantec ou a Thawte, o cliente estará pronto para SSL ou TLS e você poderá ignorar as etapas de configuração a seguir. Para obter a lista de certificados raiz da CA pré-instalados, consulte Certificados Raiz de Autoridades de Certificação.

Se o certificado não tiver sido emitido por um certificado raiz pré-instalado ou se for um certificado de autoridade de certificação interno mantido dentro de sua empresa, deve-se configurar o agente de recuperação para se comunicar com o servidor usando o protocolo TLS ou SSL.

### **Procedimento**

Para ativar a comunicação SSL ou TLS do agente de recuperação para o servidor usando um certificado de autoridade de certificação:

1. Anexe o caminho binário do GSKit e o caminho da biblioteca à variável de ambiente `PATH`. Por exemplo:

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;  
C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```
2. Se você estiver configurando SSL ou TLS no cliente pela primeira vez, deve-se criar o banco de dados de chaves do cliente local `dsmcert.kdb`. Para clientes, a

partir do diretório C:\Windows\SysWOW64, execute o comando **gsk8capicmd\_64** conforme mostrado no exemplo a seguir:

```
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
```

A senha fornecida é usada para criptografar o banco de dados de chaves. A senha é armazenada automaticamente criptografada no arquivo stash (dsmcert.sth). O arquivo stash é usado pelo cliente para recuperar a senha do banco de dados de chaves.

3. Obtenha o certificado de CA.
4. Importe o certificado para o banco de dados dsmcert.kdb. Deve-se importar o certificado de cada cliente para o dsmcert.kdb. Para clientes, a partir do diretório C:\Windows\SysWOW64, execute o comando **gsk8capicmd\_64** conforme mostrado no exemplo a seguir:

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"  
-file path_to_CA_root_certificate -format ascii -trust enable
```

Vários certificados do servidor podem ser incluídos no banco de dados dsmcert.kdb para que o cliente possa se conectar a diferentes servidores. Diferentes certificados devem ter diferentes etiquetas. Use nomes significativos para os rótulos.

**Importante:** Para uma recuperação de desastre do servidor, se o certificado tiver sido perdido, o servidor gera automaticamente um novo certificado. Cada cliente deve importar o novo certificado.

5. Após o certificado do servidor ser incluído no banco de dados dsmcert.kdb, inclua a opção `ssl yes` no arquivo C:\Windows\SysWOW64\fb.opt e atualize o valor da opção `tcpport`.

**Importante:**

O servidor geralmente é configurado para conexões SSL e TLS em uma porta diferente das conexões não SSL e TLS. Não especifique um número da porta não SSL ou TLS para o valor de `tcpport`. Se o valor de `tcpport` estiver incorreto, o agente de recuperação não poderá se conectar ao servidor.

Não é possível se conectar a uma porta não SSL ou TLS com um agente de recuperação que está ativado para SSL ou TLS ou se conectar uma porta SSL ou TLS para um agente de recuperação que não está ativado para SSL ou TLS.

6. Configure as portas SSL ou TLS corretas nos arquivos de configuração do agente de recuperação a seguir:
  - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf
  - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf

---

## Configurações do código de idioma

As configurações do código de idioma identificam o idioma que é usado para interfaces, mensagens e ajuda on-line.

### GUIs do Proteção de Dados para VMware

A frase “GUI do Proteção de Dados para VMware” se aplica às GUIs a seguir:

- GUI do Data Protection for VMware vSphere acessada em um navegador da web
- Extensão do IBM Spectrum Protect na GUI do vSphere Web Client

As GUIs do Proteção de Dados para VMware não suportam execução em um ambiente que contém configurações de código de idioma inconsistentes entre os processadores que executam a GUI do Proteção de Dados para VMware, o VMware vSphere Client e o servidor IBM Spectrum Protect.

Especifique as mesmas configurações de código de idioma entre os sistemas que executam a GUI do Proteção de Dados para VMware, o VMware vSphere Client e o servidor IBM Spectrum Protect.

Quando uma página de ajuda da GUI do Proteção de Dados para VMware for acessada por meio do link "Saiba mais" pela primeira vez, a ajuda será exibida no idioma que é especificado pela configuração do código de idioma do sistema que executa a GUI do Proteção de Dados para VMware. A ajuda não será exibida no idioma que é especificado pelo idioma do VMware vSphere Client a primeira vez que a ajuda for acessada. Nessa situação, após a página da ajuda da interface gráfica com o usuário do Proteção de Dados para VMware ser exibida, clique pelo menos em dois links dentro da ajuda, em seguida, feche a ajuda. A próxima vez que a ajuda for iniciada a partir do link "Saiba mais", ela será exibida no idioma que é especificado pela configuração do código de idioma do VMware vSphere Client.

### Interface da restauração do arquivo do IBM Spectrum Protect

O idioma do prompt de mensagens e o conteúdo da interface são determinados pela configuração de idioma do navegador da web que acessa a interface da restauração do arquivo do IBM Spectrum Protect.

Para as mensagens de erro que são registradas no arquivo `fr_api.log`, a interface da restauração do arquivo do IBM Spectrum Protect usa o idioma que é especificado pela configuração do código de idioma do sistema que executa o GUI do Data Protection for VMware vSphere.

---

## Atividade do arquivo de log

O Proteção de Dados para VMware cria e modifica vários arquivos de log durante as operações de instalação, backup, montagem e restauração.

Os arquivos de log do Proteção de Dados para VMware são arquivos de texto simples que usam uma extensão de arquivo `.sf`.

**Windows** Os logs são colocados no seguinte diretório:

`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`

Os diretórios contêm um subdiretório para cada componente do Proteção de Dados

para VMware. Por exemplo, o subdiretório do agente de recuperação é \mount; e o subdiretório da interface da linha de comandos do Recovery Agent é \shell. É possível procurar arquivos de log no menu **Iniciar do > Windows**, selecionando **Painel de Controle > Pesquisar** e inserindo \*.log.

**Linux** Os logs são colocados nestes caminhos:  
<user.home>/tivoli/tsm/ve/mount/log  
/opt/tivoli/tsm/TDPVMware/mount/engine/var  
É possível procurar arquivos de log digitando este comando:  
find /opt/tivoli/ -name "\*.log"

**Importante:** Os arquivos de log existentes são sobrescritos toda vez que uma instalação é iniciada. Se houver um problema de instalação e for necessário reinstalar o produto, recupere o arquivo TDPVMwareInstallation.log existente a partir do diretório %allusersprofile%, antes de tentar a instalação novamente.

**Nota:** Durante a execução do serviço do Proteção de Dados para VMware, vários arquivos de log são mantidos em estado aberto. Como resultado, alguns gerenciadores de arquivos não exibem o estado atual desses arquivos e podem relatar um tamanho de arquivo igual a zero. A seleção ou abertura de um desses arquivos força o gerenciador de arquivos a atualizar os detalhes do arquivo.

## Arquivos de Log do agente de recuperação

O arquivo de log do agente de recuperação é TDP\_FOR\_VMWARE\_MOUNTnnn.sf. O arquivo de log com os dados mais recentes é armazenado no arquivo de log com o número 040 (TDP\_FOR\_VMWARE\_MOUNT040.sf). Quando um arquivo de log alcança o limite de tamanho máximo, um novo arquivo de log é criado. O nome do arquivo de log é o mesmo, exceto que o número do arquivo de log diminui em um. Especificamente, os dados do arquivo de log com o número 040 são copiados para um arquivo de log com o número 039. O arquivo de log com o número 040 contém os dados do arquivo de log mais recentes. Quando 040 atinge novamente o tamanho máximo do arquivo, o conteúdo do arquivo 039 é movido para 038 e as informações de 040 vão para 039 novamente.

## Arquivos de log da GUI do Data Protection for VMware

O GUI do Data Protection for VMware vSphere coloca arquivos de log neste diretório:

**Windows** C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\logs  
**Linux** /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

Quando você estiver coletando arquivos de log, certifique-se de incluir todos os subdiretórios no arquivo compactado.

## Arquivos de Log do Interface da linha de comandos do Data Protection for VMware

O Interface da linha de comandos do Data Protection for VMware coloca arquivos de log neste diretório:

**Windows** C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\logs  
**Linux** /opt/tivoli/tsm/tdpvmware/common/logs

Quando você estiver coletando arquivos de log, certifique-se de incluir todos os subdiretórios no arquivo compactado.



## Arquivos de log da interface de restauração de arquivos do IBM Spectrum Protect

A interface de restauração de arquivos do IBM Spectrum Protect registra mensagens de erro nos arquivos `fr_api.log`, `fr_gui.log` e `messages.log`. Esses arquivos ficam no seguinte diretório padrão:

Windows	C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\logs
Linux	/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

É possível alterar o nome e o local do arquivo `fr_api.log`, configurando as opções `API_LOG_FILE_NAME` e `API_LOG_FILE_LOCATION` no arquivo da atividade de log de restauração de arquivos (`FRLog.config`).

As operações de restauração de arquivos também são registradas pelo servidor IBM Spectrum Protect. É possível procurar essas mensagens usando um cliente administrativo da linha de comandos do servidor.

- Para iniciar uma sessão de cliente administrativo no modo de linha de comando, insira este comando na estação de trabalho:

```
dsmadm -id=admin -password=admin -dataonly=yes
```

Ao inserir o comando **DSMADM** com as opções **-ID** e **-PASSWORD**, conforme mostrado, não será necessário inserir um ID e uma senha de usuário.

- Para fazer uma procura na tabela estendida de resumo de SQL para visualizar resultados sobre as operações de restauração de arquivos, emita o comando **select** a partir do cliente administrativo da linha de comandos:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
```

É possível limitar a procura, incluindo um ou mais dos seguintes critérios na instrução **SELECT**:

```
* ENTITY='DATA_MOVER_NODE_NAME'  
* AS_ENTITY='DATA_CENTER_NODE_NAME'  
* SUB_ENTITY='VM_HOST_NAME'  
* START_TIME='yyyy-MM-dd HH:mm:ss'
```

Por exemplo:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'  
and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'  
and START_TIME>'2015-03-11 17:30:00'
```

Os critérios `START_TIME` suportam consultas com os seguintes sinais: igual (=), menor que (<) ou maior que (>).

- Para fazer uma procura na tabela do log de atividades de SQL para visualizar eventos sobre as operações de restauração de arquivos, emita o comando **select** a partir do cliente administrativo da linha de comandos:

```
select * from ACTLOG
```

É possível limitar a procura incluindo um ou mais dos critérios a seguir na instrução **SELECT**:

```
* NODENAME='DATA_CENTER_NODE_NAME'  
* DATE_TIME='yyyy-MM-dd HH:mm:ss'
```

Por exemplo:

```
select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2015-03-11 17:30:00'
```

Especifique *DATA\_MOVER\_NODE\_NAME* e *DATA\_CENTER\_NODE\_NAME* em caracteres maiúsculos.

Os critérios *DATE\_TIME* suportam consultas com os seguintes sinais: igual (=), menor que (<) ou maior que (>).

---

## Iniciando e Executando Serviços para Proteção de Dados para VMware

Por padrão, quando o sistema operacional Windows é iniciado, o agente de recuperação é iniciado sob a Conta do Sistema Local.

### Executando serviços do agente de recuperação no Microsoft Windows

Ao iniciar o agente de recuperação a partir do menu Iniciar do Windows, o serviço será parado automaticamente. Quando agente de recuperação, iniciado a partir do menu Iniciar, for concluído, o serviço será iniciado automaticamente. Além disso, para esses sistemas operacionais, o serviços não fornece uma GUI. Para usar a GUI (interface gráfica com o usuário), acesse o menu Iniciar do Windows e selecione **Todos os Programas > IBM Spectrum Protect > Proteção de Dados para VMware > agente de recuperação**.

### Interface da linha de comandos do Data Protection for VMware

É possível verificar se o Interface da linha de comandos do Data Protection for VMware está em execução concluindo esta tarefa:

**Windows** Acesse **Iniciar > Painel de Controle > Ferramentas Administrativas > Serviços** e verifique se o status do Interface da linha de comandos do Data Protection for VMware é Iniciado.

**Linux** Acesse o diretório de scripts (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) e emita este comando:

```
./vmclid status
```

- Se o daemon não estiver em execução, emita este comando para iniciar o daemon manualmente:

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

Esses scripts de inicialização podem ser usados também para parar e iniciar o daemon:

```
./vmclid stop  
./vmclid start
```

---

## Apêndice A. Tarefas avançadas de configuração

Você deve configurar e verificar manualmente cada componente usando as interfaces de aplicativo disponíveis.

### Antes de Iniciar

Certifique-se de que as condições a seguir existam antes de continuar com esta tarefa:

- Um servidor IBM Spectrum Protect deve estar disponível para registrar os nós.
- O GUI do Data Protection for VMware vSphere é instalado em um sistema que atende aos pré-requisitos do sistema operacional. Ele deve ter conectividade de rede com os sistemas a seguir:
  - Servidor de Backup vStorage
  - Servidor IBM Spectrum Protect
  - vCenter Server

### Procedimento

1. Efetue logon no servidor IBM Spectrum Protect e execute as tarefas descritas em “Configurando os Nós do IBM Spectrum Protect em um Ambiente vSphere” na página 82.
2. Efetue logon no Servidor de Backup vStorage e execute as tarefas descritas em “Configurando Nós do Mover de Dados em um Ambiente vSphere” na página 83.
3. Efetue logon no sistema onde a GUI do Data Protection for VMware vSphere está instalada e conclua as tarefas descritas em “Configurando o Interface da linha de comandos do Data Protection for VMware em um ambiente do vSphere” na página 88.
4. No sistema em que o GUI do Data Protection for VMware vSphere está instalado, inicie o vSphere Client e efetue logon no vCenter. Se o vSphere Client já estiver em execução, você deverá parar e reiniciá-lo.
5. Acesse o diretório Inicial no vSphere Client. Clique no ícone GUI do Data Protection for VMware vSphere no painel Soluções e Aplicativos.

**Dica:** Se o ícone não for mostrado, então o GUI do Data Protection for VMware vSphere não foi registrado ou ocorreu um erro de conexão.

- a. No menu do vSphere Client, acesse **Plug-ins > Gerenciar Plug-ins** para iniciar o Gerenciador de Plug-in.
- b. Se for possível localizar a GUI do Data Protection for VMware vSphere e ocorrer um erro de conexão, verifique a conectividade com a máquina onde a GUI do Data Protection for VMware vSphere está instalada, emitindo o comando ping.

### Resultados

A GUI do Data Protection for VMware vSphere está pronta para operações de backup e restauração.

---

## Configurando os Nós do IBM Spectrum Protect em um Ambiente vSphere

Este procedimento descreve como registrar nós manualmente no servidor IBM Spectrum Protect e conceder autoridade de proxy para estes nós em um ambiente vSphere.

### Antes de Iniciar

**Importante:**

### Sobre Esta Tarefa

Todas as etapas neste procedimento são executadas no servidor IBM Spectrum Protect.

**Dica:** Esta tarefa também pode ser executada usando o assistente de configuração do GUI do Data Protection for VMware vSphere ou o bloco de notas de configuração de edição. Inicie o GUI do Data Protection for VMware vSphere abrindo um navegador da web e acessando ao servidor da web da GUI. Por exemplo:

<https://guihost.mycompany.com:9081/TsmVMwareUI/>

Efetue login usando o nome de usuário e a senha do vCenter.

- Para uma configuração inicial, acesse **Configuração > Executar Assistente de Configuração**.
- Para uma configuração existente, acesse **Configuração > Configuração de Edição**.

### Procedimento

1. Efetue login no servidor IBM Spectrum Protect e inicie uma sessão administrativa de cliente no modo de linha de comandos:  

```
dsmadm -id=admin -password=admin -dataonly=yes
```
2. Emita o comando **REGister Node** para registrar os nós a seguir no servidor IBM Spectrum Protect:
  - a. O nó que representa o VMware vCenter (Nó do vCenter):  

```
REGister Node MY_VCNODE <password for MY_VCNODE>
```
  - b. O nó que se comunica entre o IBM Spectrum Protect e o GUI do Data Protection for VMware vSphere (Nó do VMCLI):  

```
REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
```
  - c. O nó que representa o datacenter e é onde os dados da MV são armazenados (nó do datacenter):  

```
REGister Node MY_DCNODE <password for MY_DCNODE>
```
  - d. O nó que "move dados" de um sistema para outro (nó do movedor de dados):  

```
REGister Node MY_DMNODE <password for MY_DMNODE>
```

**Atenção:** Ao registrar nós no servidor IBM Spectrum Protect, não use o parâmetro `userid`.

3. Emita o comando **GRant PROXynode** para definir relacionamentos de proxy para estes nós:

**Lembre-se:** Os nós de destino possuem os dados e os nós do agente agem em nome dos nós de destino. Quando concedida autoridade de proxy a um nó de destino, um nó do agente pode executar operações de backup e restauração para o nó de destino.

- a. Conceda autoridade de proxy ao Nó do vCenter emitindo este comando:

```
GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

Esse comando concede a MY\_DCNODE e MY\_VMCLINODE a autoridade para fazer backup e restaurar MVs em nome de MY\_VCNODE.

- b. Conceda autoridade de proxy ao nó do datacenter emitindo este comando:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Esse comando concede a MY\_VMCLINODE e MY\_DMNODE a autoridade para fazer backup e restaurar MVs em nome de MY\_DCNODE.

- c. (Opcional) Conceda autoridade de proxy a qualquer nó do datacenter ou nó do movedor de dados adicional em seu ambiente.
- d. Verifique os relacionamentos de proxy emitindo o comando Query PROXynode do IBM Spectrum Protect. A saída de comando esperada é mostrada aqui: A saída de comando esperada é:

Nó de Destino	Nó do Agente
MY_VCNODE	MY_DCNODE MY_VMCLINODE
MY_DCNODE	MY_VMCLINODE MY_DMNODE

## O que Fazer Depois

Depois de configurar com êxito os nós do IBM Spectrum Protect, a próxima tarefa de configuração manual é configurar os nós do movedor de dados, conforme descrito em “Configurando Nós do Movedor de Dados em um Ambiente vSphere”.

---

## Configurando Nós do Movedor de Dados em um Ambiente vSphere

Se você transferir cargas de trabalho de backup para um servidor de backup vStorage em um ambiente do vSphere, configure os nós do movedor de dados para executar a operação e mover os dados para o servidor IBM Spectrum Protect.

### Antes de Iniciar

Em um ambiente Proteção de Dados para VMware padrão, uma sub-rotina do arquivo dsm.opt (Windows) ou do arquivo dsm.sys (Linux) separada é usada para cada nó do movedor de dados. Quando vários nós do movedor de dados em um vStorage Backup Server forem usados para deduplicação de dados, e esses nós tiverem autoridade para mover dados para o mesmo nó do datacenter, cada sub-rotina do arquivo dsm.opt ou arquivo dsm.sys deverá incluir um valor diferente para a opção dedupcachepath. Para obter melhores resultados, especifique uma opção schedlogname e errorlogname diferente para cada sub-rotina de arquivo dsm.opt ou arquivo dsm.sys. O conjunto mínimo de opções necessárias é fornecido na Etapa 2.

Tipicamente, o nó movedor de dados usa a SAN para fazer backup e restaurar dados. Se você configurar o nó movedor de dados para acessar os volumes de dados diretamente, desligue a designação de letra da unidade automática. Se você não desativar as designações de letra, o cliente no nó movedor de dados poderá

corromper o Raw Data Mapping (RDM) dos discos virtuais. Se o RDM dos discos virtuais for corrompido, os backups falharão. Considere as condições a seguir para as configurações de restauração:

**O nó do movedor de dados está em um sistema Windows Server:**

Se você planejar usar a SAN para restaurar dados, deverá configurar a política de SAN do Windows como `OnlineAll`. Execute `diskpart` e digite os comandos a seguir para desativar a designação de letra da unidade automática e configurar a política de SAN como **OnlineAll**:

```
diskpart
automount disable
automount scrub
san policy OnlineAll
exit
```

**O movedor de dados está instalado em uma máquina virtual em um sistema Windows Server:**

Se você planejar usar o transporte `hotadd` para restaurar dados a partir dos discos incluídos dinamicamente, a política de SAN nesse sistema também deverá ser configurada como `OnlineAll`.

Se o cliente usar a SAN ou o transporte `hotadd`, a política de SAN do Windows deverá ser configurada como `OnlineAll`. Se a política de SAN não será configurada como `OnlineAll`, as operações de restauração falharão e a mensagem a seguir será retornada:

```
ANS9365E VMware vStorage API error.
TSM function name: vddksdk Write
TSM file : vmvddksdk.cpp (2271)
API return code : 1
API error message : Unknown error
ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib_Write
FAILURE startSector=512 sectorSize=512 byteOffset=262144,
rc=-1
```

**Restrição:** O Proteção de Dados para VMware não suporta planejar o Servidor de Backup vStorage (que é usado como movedor de dados) para fazer backup de si mesmo. Certifique-se de que o Servidor de Backup vStorage seja excluído de seus próprios planejamentos. Use um Servidor de Backup vStorage diferente para executar o backup de uma MV que contenha um Servidor de Backup vStorage.

## Sobre Esta Tarefa

**Dica:** Todas as etapas nesse procedimento são executadas no Servidor de Backup vStorage.

## Procedimento

1. Atualize o arquivo de opções do movedor de dados com essas configurações:

- **Windows** Especifique estas opções no arquivo de opções `dsm.opt`.
- **Linux** Especifique estas opções no arquivo `dsm.sys`, na sub-rotina do nó do movedor de dados.

### NODENAME

Especifique o nome de um nó do movedor de dados definido anteriormente. Os planejamentos do IBM Spectrum Protect são associados ao nó do movedor de dados.

### PASSWORDACCESS

Especifique `GENERATE`, para que a senha seja gerada automaticamente (em vez de um prompt do usuário).

## VMCHOST

Especifique o nome do host do vCenter (ou servidor ESX) no qual os comandos de backup fora do host são direcionados.

## VMBACKUPTYPE

Especifique IFFULLVM. Essa configuração designa que um backup completo incremental da VM (máquina virtual) é executado. Esse valor é necessário para executar backups completos incrementais contínuos da VM (máquina virtual) e backups incrementais contínuos da VM (máquina virtual).

## MANAGEDSERVICES

Especifique esta opção para direcionar o client acceptor para gerenciar o Web client e o planejador (schedule webclient).

## TCPSERVERADDRESS

Especifique o endereço TCP/IP para o servidor IBM Spectrum Protect.

## TCPPORT

Especifique o endereço da porta TCP/IP para o servidor IBM Spectrum Protect.

## COMMMETHOD

Especifique o método de comunicação a ser usado pelo servidor IBM Spectrum Protect. Para nós do movedor de dados, você deve especificar TCP/IP como o método de comunicação. Se outro método for especificado, as operações falharão.

## HTTPPORT

Esta opção especifica um endereço de porta TCP/IP e é necessária somente quando mais de um serviço de client acceptor é usado. Por exemplo, se dois nós do movedor de dados (e dois serviços de client acceptor) forem usados, o arquivo de opções para cada nó do movedor de dados deverá especificar um valor HTTPPORT diferente.

Um arquivo dsm.dm.opt de exemplo com essas configurações é fornecido aqui:

```
NODename MY_DMNODE
PASSWORDAccess generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType Fullvm
MANAGEDServices schedule webclient
TCPServeraddress tmsserver.mycompany.xyz.com
TCPPort 1500
COMMMethod tcpip
HTTPPORT 1583
```

Para acesso instantâneo, restauração instantânea ou operações de montagem (restauração de arquivo), certifique-se de incluir VMISCSISERVERADDRESS no arquivo de opções do movedor de dados. Especifique o endereço IP do servidor iSCSI da placa de rede no vStorage Backup Server que é usado para a transferência de dados iSCSI durante operações instantâneas. A placa da interface de rede (NIC) física que está ligada ao dispositivo iSCSI no host ESX deve estar na mesma sub-rede que a NIC no vStorage Backup Server usado para a transferência iSCSI.

2. Emita esse comando para configurar o usuário e a senha do VMware vCenter para cada nó do movedor de dados:  
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
3. Inicie uma sessão da linha de comandos do movedor de dados com os parâmetros da linha de comandos -asnodename e -optfile:

```
dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
```

Certifique-se de que após a conexão inicial, sua senha não seja solicitada.

**Atenção:** Para evitar que o planejador do IBM Spectrum Protect falhe, certifique-se de que a opção `asnodename` não esteja configurada na sub-rotina do arquivo `dsm.opt` (Windows) ou do arquivo `dsm.sys` (Linux). O planejador consulta o servidor IBM Spectrum Protect para obter os planejamentos associados ao `nodename` (nó do movedor de dados), não ao `asnodename` (nó do datacenter). Se `asnodename` estiver configurado em `dsm.opt` ou `dsm.sys`, os planejamentos associados a `asnodename` (e não a `nodename`) serão consultados. Como resultado, as operações de planejamento falharão.

Conclua estas tarefas:

- a. Verifique a conexão com o servidor IBM Spectrum Protect emitindo este comando:

```
dsmc query session
```

Este comando mostra informações sobre a sessão, incluindo o nome do nó atual, quando a sessão foi estabelecida, as informações do servidor e as informações de conexão do servidor.

- b. Verifique se é possível fazer backup de uma MV emitindo este comando:

```
dsmc backup vm vm1
```

Nas Etapas 3b e 3d, `vm1` é o nome da MV.

- c. Verifique se o backup foi concluído com êxito, emitindo este comando:

```
dsmc query vm "*"
```

- d. Verifique se a MV pode ser restaurada emitindo este comando:

```
dsmc restore vm vm1 -vmname=vm1-restore
```

4. Configure o serviço de client acceptor e o serviço do planejador do movedor de dados concluindo as etapas a seguir:

- **Windows** Esse procedimento usa o assistente Configuração de GUI do Cliente do IBM Spectrum Protect para configurar o serviço de client acceptor e o serviço do planejador. Por padrão, o serviço do agente do cliente remoto também é configurado por meio do assistente. Se você usar IBM Spectrum Protect Client Service Configuration Utility (**dsmcutil**) para essa tarefa, certifique-se de também instalar o serviço do agente do cliente remoto.

Inicie o assistente de Configuração do Cliente IBM Spectrum Protect no menu de arquivo acessando **Utilitários > Assistente de Configuração**:

- Selecione **Ajude-me a configurar o TSM Web Client**. Insira as informações conforme solicitado.
  - a. Na opção Quando deseja que o serviço seja iniciado?, selecione **Automaticamente quando o Windows for inicializado**.
  - b. Na opção Gostaria de iniciar o serviço na conclusão deste assistente?, selecione **Sim**.

Quando a operação for concluída com êxito, retorne para a página de boas-vindas do assistente e prossiga para a Etapa b.

**Dica:** Ao configurar mais de um nó do movedor de dados na mesma máquina, você deve especificar um valor de porta diferente para cada instância do client acceptor.

- Selecione **Ajude-me a Configurar o TSM Client Scheduler**. Insira as informações conforme solicitado.



- a. Ao inserir o nome do planejador, certifique-se de selecionar a opção **Usar o Client Acceptor Daemon (CAD) para gerenciar o planejador.**
  - b. Na opção Quando deseja que o serviço seja iniciado?, selecione **Automaticamente quando o Windows for inicializado.**
  - c. Na opção Gostaria de iniciar o serviço na conclusão deste assistente?, selecione **Sim.**
- **Linux** Para o movedor de dados no Linux, conclua as etapas a seguir:
  - a. Especifique as opções a seguir no arquivo dsm.sys na sub-rotina para nó do movedor de dados:
    - Especifique a opção managedservices com estes dois parâmetros:  
managedservices schedule webclient

Essa configuração direciona o client acceptor para gerenciar o Web client e o planejador.

  - (Opcional) Se você desejar direcionar informações de planejamento e erro para os arquivos de log diferentes dos arquivos padrão, especifique as opções schedlogname e errorlogname com um caminho completo e nome do arquivo no qual armazenar as informações de log. Por exemplo:  

```
schedlogname /vmsched/dsmsched_dm.log
errorlogname /vmsched/dsmerror_dm.log
```
- b. Inicie o serviço de client acceptor:
 

O programa de instalação cria um script de inicialização para o client acceptor (dsmcad) em /etc/init.d. O client acceptor deve ser iniciado para que possa gerenciar tarefas do planejador ou o Web client. Como raiz, conclua as etapas a seguir:

  - 1) Configure o serviço de client acceptor e o serviço do planejador do movedor de dados para agirem como um Servidor de Backup vStorage. Deve-se configurar a variável de ambiente LD\_LIBRARY\_PATH para o diretório de instalação do cliente e a biblioteca compartilhada Java libjvm.so. O caminho para o libjvm.so também é usado para suporte à identificação quando você ativa a opção do cliente vmtagdatamover no movedor de dados.

Assegure-se de que o software Java esteja instalado e a variável de ambiente JAVA\_HOME seja exportada corretamente.

Os caminhos a seguir são exemplos típicos do caminho para libjvm.so:

  - Para IBM Java: \$JAVA\_HOME/jre/bin/classic/libjvm.so
  - Para Oracle Java: \$JAVA\_HOME/jre/lib/amd64/server/libjvm.so

Deve-se configurar a variável de ambiente LD\_LIBRARY\_PATH no arquivo /etc/init.d/dsmcad. Por exemplo:

  - Para IBM Java, configure a variável de ambiente a seguir:  

```
export
LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic/
```
  - Para Oracle Java, configure a variável de ambiente a seguir:  

```
export
LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server/
```
  - 2) Inicie o client acceptor emitindo o seguinte comando:  

```
service dsmcad start
```

Para permitir que o client acceptor seja iniciado automaticamente após uma reinicialização do sistema, inclua o serviço da seguinte forma em um prompt de shell:

```
# chkconfig --add dsmscad
```

**Dica:** Se desejar executar o comando **dsmsc** diretamente a partir da linha de comandos do Linux, também deve-se aplicar a variável de ambiente LD\_LIBRARY\_PATH ao shell de comando.

5. Verifique se o client acceptor e o agente estão configurados corretamente:
  - a. Efetue login em um sistema remoto.
  - b. Use um navegador da web para se conectar ao sistema HOST1 usando este endereço e porta:  
`http://HOST1.xyz.yourcompany.com:1581`

**Dica:** Quando o endereço IP é alterado no sistema em que o GUI do Data Protection for VMware vSphere está instalado, você deve executar o seguinte:

- a. Configure o client acceptor novamente (Etapa 3) para que o GUI do Data Protection for VMware vSphere seja ativado para operações. Caso contrário, o Gerenciador de Plug-in mostrará o status do GUI do Data Protection for VMware vSphere como desativado.

## O que Fazer Depois

Depois de configurar com êxito os nós do movedor de dados, a próxima tarefa de configuração manual é configurar o perfil VMCLI conforme descrito em “Configurando o Interface da linha de comandos do Data Protection for VMware em um ambiente do vSphere”.

---

## Configurando o Interface da linha de comandos do Data Protection for VMware em um ambiente do vSphere

Atualize o perfil do Interface da linha de comandos do Data Protection for VMware no sistema em que o GUI do Data Protection for VMware vSphere está instalado.

### Antes de Iniciar

O perfil (vmcliprofile) está localizado neste diretório no sistema em que o GUI do Data Protection for VMware vSphere está instalado:

```
Linux /opt/tivoli/tsm/tdpvmware/common/scripts
```

```
Windows 64 bits: C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts
```

### Sobre Esta Tarefa

Todas as etapas neste procedimento são concluídas no sistema em que o GUI do Data Protection for VMware vSphere está instalado.

**Dica:** Esta tarefa também pode ser executada usando o assistente de configuração do GUI do Data Protection for VMware vSphere ou o bloco de notas de

configuração. Acesse a janela Configuração do GUI do Data Protection for VMware vSphere e clique em **Assistente de configuração de execução** ou **Configuração de edição**.

## Procedimento

1. Atualize o perfil com estas configurações:

### VE\_TSMCLI\_NODE\_NAME

Especifique o nó que conecta o Interface da linha de comandos do Data Protection for VMware ao servidor IBM Spectrum Protect e ao nó do agente (MY\_VMCLINODE).

**Restrição:** O Nó do VMCLI não suporta protocolo SSL ou autenticação LDAP ao comunicar-se com o servidor IBM Spectrum Protect.

### VE\_VCENTER\_NODE\_NAME

Especifique o nó virtual que representa um vCenter (MY\_VCNODE).

### VE\_DATACENTER\_NAME

Especifique o nó virtual mapeado para um datacenter. A sintaxe correta é mostrada aqui:

datacenter\_name::datacenter\_node\_name

- O valor datacenter\_name faz distinção entre maiúsculas e minúsculas.
- Certifique-se de ter configurado esse parâmetro para cada datacenter em seu ambiente (MY\_DCNODE).
- O GUI do Data Protection for VMware vSphere não suporta datacenters com o mesmo nome no vCenter.

### VE\_TSM\_SERVER\_NAME

Especifique o nome do host ou o IP do servidor IBM Spectrum Protect.

### VE\_TSM\_SERVER\_PORT

Especifique o nome da porta a ser usada para o servidor IBM Spectrum Protect. O valor padrão é 1500.

Um perfil de exemplo com estas configurações é fornecido aqui:

VE_TSMCLI_NODE_NAME	MY_VMCLINODE
VE_VCENTER_NODE_NAME	MY_VCNODE
VE_DATACENTER_NAME	MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME	tsmsrvr.mycompany.xyz.com
VE_TSM_SERVER_PORT	1500

2. Configure a senha do Nó do VMCLI no arquivo pwd.txt.

Essa senha é para o nó que conecta o Interface da linha de comandos do Data Protection for VMware ao servidor IBM Spectrum Protect e ao nó do movedor de dados. Ele é especificado pelo parâmetro de perfil VE\_TSMCLI\_NODE\_NAME.

- a. Emita o comando echo para criar um arquivo de texto que contenha a senha:

**Linux** echo password1 > pwd.txt

**Windows** echo password1> pwd.txt

**Windows** Não deve existir espaços entre a senha (password1) e o sinal de maior que (>).

- b. Emita este comando vmcli para configurar a senha para o Nó do VMCLI:  
vmcli -f set\_password -I pwd.txt

### Importante:

- **Linux** Você deve emitir o comando `vmcli -f set_password` como usuário do `tdpvmware` e não como `root`.
- **Linux** **Windows** Se você planeja gerar relatórios de proteção de aplicativo, deve especificar o parâmetro **-type VMGuest** para identificar se a senha se aplica a uma VM. Por exemplo:

```
vmcli -f set_password -type VMGuest -I password.txt
```

3. Verifique se o Interface da linha de comandos do Data Protection for VMware está em execução:

**Windows** Clique em **Iniciar > Painel de Controle > Ferramentas administrativas > Serviços** e verifique se o status do Interface da linha de comandos do Data Protection for VMware é Iniciado.

**Linux** Acesse o diretório de scripts (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) e emita este comando:

```
./vmclid status
```

- Se o daemon estiver em execução, comece a Etapa 4.
- Se o daemon não estiver em execução, emita este comando para iniciar o daemon manualmente:

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

Esses scripts de inicialização podem ser usados também para parar e iniciar o daemon:

```
./vmclid stop  
./vmclid start
```

4. Emita este comando `vmcli` para verificar se o Interface da linha de comandos do Data Protection for VMware reconhece a configuração do nó IBM Spectrum Protect:

```
vmcli -f inquire_config -t TSM
```

5. Valide os nós para confirmar se nenhum erro de configuração ocorreu:
  - a. Inicie o GUI do Data Protection for VMware vSphere clicando no ícone na janela Soluções e Aplicativos do vSphere Client.
  - b. Acesse a janela Configuração.
  - c. Selecione um nó na tabela e clique em **Validar Nó Selecionado**. São mostradas informações de status na área de janela Detalhes de Status.

## O que Fazer Depois

**Linux** **Windows** Após a conclusão bem-sucedida das três tarefas de configuração manual descritas nesta seção:

1. “Configurando os Nós do IBM Spectrum Protect em um Ambiente vSphere” na página 82
2. “Configurando Nós do Movedor de Dados em um Ambiente vSphere” na página 83

Nenhuma das tarefas adicionais de configuração são necessárias para fazer backup dos dados de sua VM.

---

## Lista de Verificação de Configuração da Interface da Linha de Comandos do Ambiente vSphere

Use este procedimento para configurar o Proteção de Dados para VMware em um ambiente vSphere usando apenas uma interface da linha de comandos.

### Procedimento

Execute a Etapa 1 e Etapa 2 no servidor IBM Spectrum Protect.

1. Registre os nós a seguir no servidor IBM Spectrum Protect:

- a. O nó que representa o VMware vCenter (Nó do vCenter):

```
REGister Node MY_VCNODE <password for MY_VCNODE>
```

- b. O nó que se comunica entre o IBM Spectrum Protect e o GUI do Data Protection for VMware vSphere (Nó do VMCLI):

```
REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
```

- c. O nó que representa o datacenter e é onde os dados da MV são armazenados (nó do datacenter):

```
REGister Node MY_DCNODE <password for MY_DCNODE>
```

- d. O nó que "move dados" de um sistema para outro (nó do movedor de dados):

```
REGister Node MY_DMNODE <password for MY_DMNODE>
```

2. Defina os relacionamentos de proxy para estes nós:

- a. Conceda autoridade de proxy ao Nó do vCenter emitindo este comando:

```
GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

Esse comando concede a MY\_DCNODE e MY\_VMCLINODE a autoridade para fazer backup e restaurar MVs em nome de MY\_VCNODE.

- b. Conceda autoridade de proxy ao nó do datacenter emitindo este comando:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Esse comando concede a MY\_VMCLINODE e MY\_DMNODE a autoridade para fazer backup e restaurar MVs em nome de MY\_DCNODE.

- c. (Opcional) Conceda autoridade de proxy a qualquer nó do datacenter ou nó do movedor de dados adicional em seu ambiente.

- d. Verifique os relacionamentos de proxy emitindo o comando Query PROXynode do IBM Spectrum Protect. A saída de comando esperada é mostrada aqui:

Nó de Destino	Nó do Agente
MY_VCNODE	MY_DCNODE MY_VMCLINODE
MY_DCNODE	MY_VMCLINODE MY_DMNODE

Execute as Etapas de 3 a 9 no Servidor de Backup vStorage.

3. Configure os valores apropriados para as opções a seguir do movedor de dados:

- Windows** Especifique estas opções no arquivo de opções dsm.opt.
- Linux** Especifique estas opções no arquivo dsm.sys, na sub-rotina do nó do movedor de dados.

```
NODENAME  
PASSWORDACCESS  
VMCHOST
```

VMBACKUPTYPE  
MANAGEDSERVICES  
TCPSEVERADDRESS  
TCPPOINT  
COMMMETHOD  
HTTPPORT

**Nota:** O HTTPPORT é necessário quando mais de um Client Acceptor Service (CAD) é usado. Por exemplo, se houver dois nós do movedor de dados (e dois serviços CAD), o arquivo de opções de cada nó do movedor de dados deverá especificar um valor HTTPPORT diferente.

Um arquivo dsm.dm.opt de exemplo com essas opções é fornecido aqui:

```
NODename MY_DMNODE  
PASSWORDAccess generate  
VMCHost vcenter.storage.usca.example.com  
VMBACKUPType Fullvm  
MANAGEDServices schedule webclient  
TCPSeveraddress tsmserver.mycompany.xyz.com  
TCPPoint 1500  
COMMMethod tcpip  
HTTPPORT 1583
```

4. Verifique a conexão com o servidor IBM Spectrum Protect emitindo este comando:  
dsmc query session
5. Emita esse comando para configurar o usuário e a senha do VMware vCenter para o nó do movedor de dados:  
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator>  
<password1>
6. Configure os serviços do IBM Spectrum Protect a seguir:
  - **Windows**
    - a. Instale o Scheduler Service:  
dsmcutil install scheduler /name:"TSM Central Scheduler Service"  
/node:MY\_DMNODE /password:MY\_DMNODEPWD /startnow:no /autostart:no
    - b. Instale o CAD:  
dsmcutil install cad /name:"TSM CAD - MY\_DMNODE" /node:MY\_DMNODE  
/password:MY\_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt  
/cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
    - c. Instale o Remote Client Agent Service:  
dsmcutil install remoteagent /name:"TSM AGENT" /node:MY\_DMNODE  
/password:MY\_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt  
/partnername:"TSM CAD - MY\_DMNODE" /startnow:no
  - **Linux** Especifique a opção managedservices no arquivo dsm.sys, na sub-rotina para o nó do movedor de dados:  
Certifique-se de especificar os parâmetros schedule e webclient:  
managedservices schedule webclient  
  
Esta configuração direciona o client acceptor a gerenciar o web client e o planejador.
7. **Linux** Para configurar o Client Acceptor Service e o Serviço do Planejador do Movedor de Dados para agir como um Servidor de Backup do vStorage, configure a seguinte variável de ambiente no arquivo /etc/init.d/dsmcad:  
export LD\_LIBRARY\_PATH=/opt/tivoli/tsm/client/ba/bin
8. **Linux** Inicie o Client Acceptor Service: O programa de instalação cria um script de inicialização para o client acceptor daemon (dsmcad) em /etc/init.d.

O client acceptor daemon deve ser iniciado para que possa gerenciar as tarefas do planejador ou gerenciar o web client. Como raiz, use o comando a seguir para iniciar o daemon:

```
service dsmcad start
```

Para ativar o Client Acceptor Daemon para ser iniciado automaticamente após uma reinicialização do sistema, inclua o serviço da seguinte forma no prompt de shell:

```
# chkconfig --add dsmcad
```

9. Verifique se os serviços do IBM Spectrum Protect estão configurados corretamente:
  - a. Efetue logon em um sistema remoto.
  - b. Use um navegador da web para se conectar ao sistema HOST1 usando este endereço e porta:  
`http://HOST1.xyz.yourcompany.com:1581`

Conclua a Etapa 10 no sistema em que o GUI do Data Protection for VMware vSphere está instalado.

10. Configure os valores apropriados para as opções a seguir no perfil do Interface da linha de comandos do Data Protection for VMware (vmcliprofile):

```
VE_TSMCLI_NODE_NAME  
VE_VCENTER_NODE_NAME  
VE_DATACENTER_NAME  
VE_TSM_SERVER_NAME  
VE_TSM_SERVER_PORT
```

Um perfil de exemplo com estas opções é fornecido aqui:

VE_TSMCLI_NODE_NAME	MY_VMCLINODE
VE_VCENTER_NODE_NAME	MY_VCNODE
VE_DATACENTER_NAME	MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME	tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT	1500

O perfil estas nos diretórios a seguir:

**Linux** /opt/tivoli/tsm/tdpvmware/common/scripts

**Windows** 64 bits: C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts

- a. Configure a senha para o Nó do VMCLI:
  - 1) Emita o comando echo para criar um arquivo de texto que contenha a senha:

**Linux**

```
echo password1 > pwd.txt
```

**Windows**

```
echo password1> pwd.txt
```

- 2) Emita este comando vmcli para configurar a senha para o Nó do VMCLI:

**Importante:** **Linux** Você deve emitir esse comando como usuário tdpvmware, não como raiz.

```
vmcli -f set_password -I pwd.txt
```

- b. Verifique se o Interface da linha de comandos do Data Protection for VMware está em execução:

**Windows** Emita esse comando em um prompt de comandos do Windows:  
`net start`

**Linux** Emita este comando:  
`./vmcliid status`

- c. Emita este comando vmcli para verificar se o Interface da linha de comandos do Data Protection for VMware reconhece a configuração do nó IBM Spectrum Protect:

```
vmcli -f inquire_config -t TSM
```

---

## Diretrizes de Configuração de Fita

Revise estas diretrizes antes de tentar operações de backup para armazenamento em fita.

### Preparando para o backup na fita

**Linux** **Windows** Antes de tentar um backup em fita, estes parâmetros devem ser configurados no servidor IBM Spectrum Protect para os backups em fita:

1. Defina a classe de gerenciamento:

```
define mgmtclass <domain name> <policy set name> <mgmtclass name>
```

Por exemplo:

```
define mgmtclass tape tape DISK
```

2. Defina o grupo de cópias:

```
define copygroup <domain name> <policy set name> <mgmtclass name>  
destination=<stgpool name>
```

Por exemplo:

```
define copygroup tape tape DISK destination=Diskpool
```

3. Ative o conjunto de políticas:

```
activate policyset <domain name> <policy set name>
```

Por exemplo:

```
activate policyset tape tape
```

Ao configurar o backup na fita física, haverá requisitos de configuração adicionais. Você deve sempre manter os metadados (arquivos de controle) do IBM Spectrum Protect no disco e os dados de backup da MV reais na fita.

- Use a opção VMCMC para armazenar os backups do VMware (e arquivos de controle do VMware) com uma classe de gerenciamento diferente da classe de gerenciamento padrão.
- Use a opção VMCTLMC para especificar a classe de gerenciamento a ser usada especificamente para arquivos de controle do VMware durante backups do VMware. A classe de gerenciamento especificada substituirá a classe de gerenciamento padrão. Ela também substituirá a classe de gerenciamento



especificada pela opção VMMC. A classe de gerenciamento VMCTLMC deve especificar um conjunto de armazenamentos em disco, sem migração para fita.

- A opção VMMC é sempre usada para controlar a retenção em backups da MV. Essa opção se aplica a configurações em disco e em fita. A opção VMCTLMC não é usada para a retenção dos arquivos de controle. Os arquivos de controle e dados fazem parte do mesmo agrupamento e expiram juntos com base na política de retenção da opção VMMC. Quando as duas opções são configuradas, VMMC é usado para arquivos de dados e VMCTLMC é usado para arquivos de controle.

**Restrição:** As operações de restauração que usam agentes de armazenamento em configurações sem a LAN podem restaurar arquivos de um conjunto de armazenamento de cópia mesmo que os dados possam ser recuperados de um conjunto de armazenamentos primários. Isso pode acontecer se a solicitação de restauração for para um arquivo específico, ou a solicitação de restauração não estiver usando o método sem consulta e a cópia primária do arquivo estiver armazenada em um conjunto de armazenamentos que não seja acessível através do caminho sem a LAN. Isso também pode afetar as situações sem restauração, como as operações de backup do Proteção de Dados para VMware. Em um ambiente do Proteção de Dados para VMware, o método de armazenamento preferencial para arquivos de controle de MV é o disco, de modo que uma montagem não precise restaurar o arquivo durante o processo de backup incremental. Esses arquivos de controle de MV não precisam apenas ser colocados no disco, porém não é necessário fazer backup deles para um conjunto de armazenamento de cópia disponível através de um caminho sem a LAN. Se isso for feito, uma montagem da fita será usada para restaurar os arquivos durante um backup incremental sem a LAN a partir de um cliente Proteção de Dados para VMware.

Se o ambiente do servidor IBM Spectrum Protect usar disco para migração em fita, considere as diretrizes a seguir antes da migração:

- Configure o conjunto de armazenamento em disco MIGDELAY com um valor que suporte a maioria das solicitações de montagem do disco a serem satisfeitas. Os padrões de uso típico indicam que uma alta porcentagem de recuperações de arquivos individuais ocorre em poucos dias. Por exemplo, de 3 a 5 dias normalmente, da hora em que um arquivo foi modificado pela última vez. Portanto, tente manter os dados em disco por esse breve período para otimizar as operações de recuperação.

Além disso, se a deduplicação do lado do cliente estiver sendo usada com o conjunto de armazenamentos em disco, configure a opção MIGDELAY que acomoda os backups completos frequentes da MV. Não migre dados do conjunto de armazenamentos deduplicado para fita até que pelo menos dois backups completos tenham sido feitos para uma MV. Quando os dados são movidos para a fita, eles não são mais deduplicados. Por exemplo, se backups completos forem executados semanalmente, considere configurar MIGDELAY para um valor de pelo menos 10 dias. Essa configuração assegura que cada backup completo identifique e use dados duplicados do backup anterior antes de ser movido para fita.

- Use um conjunto de armazenamento de arquivo de classe de dispositivo em vez de um conjunto de armazenamento de classe de dispositivo DISK. Um valor típico para um tamanho de volume, especificado por um parâmetro MAXCAPACITY de classe de dispositivo, seria de 8 GB e 16 GB. Para o conjunto de armazenamentos associado, considere aplicar a disposição por espaço no arquivo. Cada MV cujo backup é feito é representada como um espaço no arquivo separado no servidor IBM Spectrum Protect. A disposição por espaço no arquivo salva os dados de vários backups incrementais para uma determinada

MV no mesmo volume (arquivo de disco). Quando a migração em fita ocorre, a disposição por espaço no arquivo localiza diversos backups incrementais por uma determinada MV juntos em uma fita física.

Use o diálogo **Configurações** para configurar o valor do Modo de Fita.

Uma operação de backup torna-se interrompida quando uma operação de montagem ou de restauração instantânea exige o mesmo armazenamento em fita simultaneamente em uso pela operação de backup.

---

## Configurando manualmente um dispositivo iSCSI em um sistema Linux

### Linux

Este procedimento descreve como configurar um sistema Linux usado durante uma operação de montagem de iSCSI. A captura instantânea da MV é montada a partir do armazenamento do servidor IBM Spectrum Protect.

### Antes de Iniciar

Durante uma montagem de iSCSI, um destino iSCSI é criado no sistema Recovery Agent. O Microsoft iSCSI Initiator não é requerido no sistema Recovery Agent.

**Dica:** O Open-iSCSI Initiator é fornecido com o Red Hat Enterprise Linux e SUSE Linux Enterprise Server.

Revise os requisitos de iSCSI a seguir antes de prosseguir com esta tarefa:

- É possível conectar-se ao destino iSCSI a partir de qualquer sistema para criar um volume que contenha os dados de backup. É possível montar esse volume a partir de outro sistema.
- Um inicializador iSCSI é requerido em qualquer sistema que deva se conectar ao destino iSCSI.
- Um inicializador iSCSI deve ser instalado no sistema no qual os dados devem ser restaurados.
- Se um volume estender vários discos, você deverá montar todos os discos necessários. Quando os volumes espelhados forem usados, monte apenas um dos discos espelhados. A montagem de um disco evita uma operação de sincronização demorada.

### Sobre Esta Tarefa

Conclua estas etapas para configurar o sistema Linux usado durante uma operação de montagem de iSCSI:

### Procedimento

1. Registre o nome do inicializador iSCSI no sistema no qual os dados devem ser restaurados. O nome do inicializador iSCSI está localizado no arquivo `/etc/iscsi/initiatorname.iscsi`. Se o valor de `InitiatorName=` estiver vazio, crie um nome de inicializador com o comando a seguir:

```
twauslbpoc01:~ # /sbin/iscsi-iname
```

Aqui está um nome de inicializador de exemplo:

```
iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

2. Inclua o nome do inicializador para o arquivo `/etc/iscsi/initiatorname.iscsi`.
  - a. Edite o arquivo `/etc/iscsi/initiatorname.iscsi` com o comando **vi**. Por exemplo:  
`twauslbpoc01:~ # vi /etc/iscsi/initiatorname.iscsi`
  - b. Atualize o parâmetro **InitiatorName=** com o nome do inicializador. Por exemplo:  
`InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0`
3. Conclua as seguintes etapas no sistema em que o agente de recuperação (ou o destino iSCSI) está instalado:
  - a. Iniciar o agente de recuperação. Conclua os diálogos Selecionar servidor IBM Spectrum Protect e Selecionar captura instantânea e clique em **Montar**.
  - b. No diálogo Escolher Destino de Montagem, selecione Montar um Destino de iSCSI.
  - c. Crie um nome de destino. Certifique-se de que ele seja exclusivo e de que seja possível identificá-lo no sistema que executa o inicializador iSCSI. Por exemplo:  
`iscsi-mount-tsm4ve`
  - d. Insira o nome do Inicializador iSCSI que foi registrado na Etapa 1 e clique em **OK**.
  - e. Verifique se o volume que acabou de ser montado é exibido no campo Volumes Montados.
4. Localize e inicie o programa do Inicializador iSCSI no sistema do inicializador que foi selecionado na Etapa 1:
  - a. Verifique se o serviço iSCSI está em execução emitindo este comando:  
 Red Hat Enterprise Linux:  
`service iscsi status`  
  
 SUSE Linux Enterprise Server:  
`service open-iscsi status`  
  
 Se o serviço não estiver sendo executado, a emissão deste comando iniciará o serviço:  
 Red Hat Enterprise Linux:  
`service iscsi start`  
  
 SUSE Linux Enterprise Server:  
`service open-iscsi start`
  - b. Conecte-se ao destino iscsi emitindo este comando:  
`iscsiadm -m discovery -t sendtargets -p <IP/hostname of agente de recuperação system> --login`
  - c. Verifique se um novo dispositivo bruto está disponível emitindo este comando:  
`fdisk -l`
5. Monte o sistema de arquivos:  
 Para um volume não LVM, emita os comandos a seguir. Neste exemplo, o novo dispositivo é `/dev/sdb1`:  
`mkdir /mountdir`  
`mount /dev/sdb1 /mountdir`

Para um volume LVM, conclua as tarefas a seguir no convidado do Linux:

- a. Certifique-se de que o script `vgimportclone` esteja disponível no sistema Linux. Esse script não é enviado no pacote LVM base (padrão). Como resultado, você pode precisar atualizar o pacote LVM para um nível que forneça esse script.
  - b. Emita o comando **vgimportclone** e inclua um novo nome do grupo de volumes de base (`VolGroupSnap01`). Por exemplo:  

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```
  - c. Emita o comando **lvchange** para marcar o volume lógico como ativo. Por exemplo:  

```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```
  - d. Emita estes comandos para montar o volume:  

```
mkdir /mountdir  
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```
6. Após a conclusão da operação de restauração de arquivo, emita estes comandos:
- Para um volume não LVM, emita os comandos a seguir:
    - a. Desmonte o sistema de arquivos:  

```
umount /dev/sdb1 /mountdir
```
    - b. Remova o volume. Se o volume fizer parte de um grupo de volumes, primeiro remova o volume do grupo de volumes emitindo o comando a seguir:  

```
vgreduce <your_volume_group> /dev/sdb1
```

Em seguida, emita este comando para remover o volume:  

```
pvremove /dev/sdb1
```
    - c. Efetue logout de um único destino:  

```
iscsiadm --mode node --targetname <target_name> --logout
```
    - d. Efetue logout de todos os destinos:  

```
iscsiadm --mode node --logout
```
  - Para um volume LVM, conclua as tarefas a seguir no convidado do Linux:
    - a. Desmonte o sistema de arquivos:  

```
umount /mountdir
```
    - b. Remover o volume lógico:  

```
lvm lvremove LogVol00
```
    - c. Remover o grupo de volumes:  

```
lvm vgremove VolGroupSnap01
```
    - d. Efetue logout de um único destino:  

```
iscsiadm --mode node --targetname <target_name> --logout
```
    - e. Efetue logout de todos os destinos:  

```
iscsiadm --mode node --logout
```

---

# Configurando manualmente um dispositivo iSCSI em um sistema Windows

## Windows

Esse procedimento descreve como configurar um sistema Windows que é usado durante uma operação de montagem iSCSI. A captura instantânea é montada no armazenamento do servidor IBM Spectrum Protect.

### Antes de Iniciar

Revise os requisitos de iSCSI a seguir antes de continuar com esta tarefa:

- Durante uma montagem do iSCSI, um destino iSCSI é criado no sistema agente de recuperação. É possível conectar-se ao destino iSCSI a partir de qualquer sistema para criar um volume que contenha os dados de backup. Além disso, é possível, em seguida, montar este volume a partir de outro sistema.
- O inicializador iSCSI é requerido em qualquer sistema que deve se conectar ao destino iSCSI.
- Certifique-se de que um inicializador iSCSI esteja instalado no sistema no qual os dados devem ser restaurados.
- O Inicializador iSCSI da Microsoft não é requerido no sistema agente de recuperação.

Revise os requisitos de disco e volume a seguir antes de continuar com esta tarefa:

- Se um volume abranger vários discos, deve-se montar todos os discos necessários. Quando volumes espelhados são usados, monte somente um dos discos espelhados. A montagem de um disco evita uma operação de sincronização demorada.
- Se vários discos dinâmicos forem usados no sistema de backup, estes discos serão designados ao mesmo grupo. Como resultado, o Windows Disk Manager pode considerar alguns discos como ausentes e emitir uma mensagem de erro quando você monta somente um disco. Ignore esta mensagem. Os dados no disco submetido a backup ainda estão acessíveis, a menos que alguns dos dados estejam no outro disco. Este problema pode ser resolvido montando todos os discos dinâmicos.

### Sobre Esta Tarefa

Conclua estas tarefas para configurar o sistema Windows que é usado durante uma operação de montagem iSCSI:

### Procedimento

1. No sistema agente de recuperação, abra a porta 3260 no firewall da rede local e o firewall do cliente Windows. Registre o nome do inicializador iSCSI no sistema no qual os dados devem ser restaurados.  
O nome do inicializador iSCSI é mostrado na janela de configuração do inicializador iSCSI do Painel de Controle. Por exemplo:  
`iqn.1991-05.com.microsoft:hostname`
2. Execute estas tarefas no sistema no qual o agente de recuperação (ou o destino de iSCSI) está instalado:
  - a. Inicie a GUI do agente de recuperação. Conclua os diálogos Selecionar servidor IBM Spectrum Protect e Selecionar captura instantânea e clique em **Montar**.

- b. No diálogo Escolher Destino de Montagem, selecione **Montar um Destino de iSCSI**.
- c. Crie um nome de destino. Certifique-se de que ele seja exclusivo e de que seja possível identificá-lo no sistema que executa o inicializador iSCSI. Por exemplo:  
iscsi-mount-tsm4ve
- d. Insira o nome do Inicializador iSCSI que foi registrado na Etapa 1 e clique em **OK**.
- e. Verifique se o volume que acabou de ser montado é exibido no campo Volumes Montados.
- f. Quando você usa o Recovery Agent em uma rede iSCSI e ele não usa um movedor de dados, acesse C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf file e especifique a tag [IMOUNT] e o parâmetro **Target IP**:  
[IMOUNT config]  
Target IP=<IP address of the network card on the system that exposes the iSCSI targets.>

Por exemplo:

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

Após incluir ou alterar o parâmetro Target IP, reinicie a GUI do Recovery Agent ou a CLI do Recovery Agent.

- 3. Localize e inicie o programa do Inicializador iSCSI no sistema do inicializador que foi selecionado na Etapa 1:
  - a. Conecte-se ao destino iscsi:
    - 1) Na guia Destinos, insira o endereço TCP/IP do agente de recuperação (destino de iSCSI) usado na Etapa 2 no diálogo Destino:. Clique em **Conexão Rápida**.
    - 2) O diálogo Conexão Rápida mostra um destino que corresponde ao nome de destino especificado na Etapa 2c. Se ele ainda não estiver conectado, selecione este destino e clique em **Conectar**.
  - b. No sistema inicializador, acesse **Painel de Controle > Ferramentas Administrativas > Computer Management > Storage > Disk Management**.
    - 1) Se o destino de iSCSI montado for listado como Type=Foreign, clique com o botão direito do mouse em **Disco Estrangeiro** e selecione **Importar Discos Estrangeiros**. O Grupo de Disco Estrangeiro é selecionado. Clique em **OK**.
    - 2) A próxima tela mostra o tipo, a condição e o tamanho do Disco Estrangeiro. Clique em **OK** e aguarde até que o disco seja importado.
    - 3) Quando a importação do disco for concluída, pressione **F5** (atualizar). A captura instantânea de iSCSI montada é visível e contém uma letra da unidade designada. Se as letras da unidade não forem designadas automaticamente, clique com o botão direito do mouse na partição necessária e selecione **Alterar Letras da Unidade ou Caminhos**. Clique em **Incluir** e selecione uma letra da unidade.
- 4. Abra o Windows Explorer (ou outro utilitário) e procure a captura instantânea montada para uma operação de restauração de arquivo.

5. Após o arquivo ser restaurado, conclua estas tarefas:
  - a. Desconecte cada destino iscsi usando o diálogo Propriedades do Inicializador iSCSI.
  - b. Desmonte o volume a partir da Etapa 2 selecionando o volume na interface gráfica com o usuário do agente de recuperação e clicando em **Desmontar**.

---

## Configurando manualmente o nós do proxy de montagem em um sistema Linux

### Linux

Conclua esta tarefa para incluir um nó do proxy de montagem em um sistema Linux remoto.

### Antes de Iniciar

Em um ambiente do GUI do Data Protection for VMware vSphere padrão, uma sub-rotina do arquivo `dsm.sys` separada é usada para cada nó do proxy de montagem. Todas as etapas neste procedimento são concluídas usando o movedor de dados instalado no servidor de backup.

### Sobre Esta Tarefa

Esta tarefa configura o nós do proxy de montagem atualizando as opções do movedor de dados e verificando a conectividade com o servidor IBM Spectrum Protect.

### Procedimento

1. Especifique estas opções no arquivo `dsm.sys`, na sub-rotina do nó do proxy de montagem.

#### NODENAME

Especifique o nome de um nó do proxy de montagem definido anteriormente. Os planejamentos do IBM Spectrum Protect são associados a este nó.

#### PASSWORDACCESS

Especifique `GENERATE`, para que a senha seja gerada automaticamente (em vez de um prompt do usuário).

#### MANAGEDSERVICES

Especifique esta opção para direcionar o client acceptor para gerenciar o Web client e o planejador (Web client de planejamento).

#### TCPSERVERADDRESS

Especifique o endereço TCP/IP para o servidor IBM Spectrum Protect.

#### TCPPORT

Especifique o endereço da porta TCP/IP para o servidor IBM Spectrum Protect.

#### COMMMETHOD

Especifique o método de comunicação que será usado pelo servidor IBM Spectrum Protect. Para nós do proxy de montagem, deve-se especificar Protocolo de Controle de Transmissões/Protocolo da Internet como o método de comunicação. As operações falharão se outro método for especificado.

## HTTPPORT

Esta opção especifica um endereço de porta TCP/IP e deve ser especificada somente quando mais de um Client Acceptor Service (CAD) é usado. Por exemplo, se houver dois nós do proxy de montagem (e dois serviços CAD), o arquivo de opções para cada nó do proxy de montagem deverá especificar um valor de HTTPPORT diferente.

**Restrição:** Não ative a opção sem a LAN (ENABLELANFREE YES) no arquivo dsm.sys. Essa opção não é suportada para montagem de nós do proxy. Um arquivo dsm.sys de exemplo com estas configurações é fornecido aqui:

```
Servername      tsm_server1
NODename datacenter1_MP_LNX
PASSWORDAccess generate
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.myco.com
TCPPort 1500
COMMMethod tcpip
HTTPPORT 1583
```

2. Emita este comando para configurar o usuário e a senha do VMware vCenter para o nó do proxy de montagem:  
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator>  
<password1>

3. Inicie uma sessão da linha de comandos do movedor de dados com os parâmetros da linha de comandos -asnodername e -optfile:  
dsmc -asnodername=vctr1\_datacenter1 -optfile=dsm\_MP\_LNX.sys  
Certifique-se de que após a conexão inicial, sua senha não seja solicitada.

**Atenção:** Para evitar a falha do planejador do IBM Spectrum Protect, certifique-se de que a opção asnodename não esteja configurada na sub-rotina do arquivo dsm.sys (Linux). O planejador consulta o servidor IBM Spectrum Protect para obter os planejamentos associados ao nodename (nó do proxy de montagem), não ao asnodename (nó do datacenter). Se asnodename estiver configurado em dsm.sys, planejamentos que estão associados a asnodename (e não a nodename) serão consultados. Como resultado, as operações de planejamento falharão.

4. Verifique a conexão com o servidor IBM Spectrum Protect emitindo este comando:

```
dsmc query session
```

Este comando mostra informações sobre a sessão, incluindo o nome do nó atual, quando a sessão foi estabelecida, as informações do servidor e as informações de conexão do servidor.

5. Configure o Client Acceptor Service (CAD) e o Serviço do Planejador do Mover de Dados concluindo estas tarefas:

- Especifique estas opções no arquivo dsm.sys, na sub-rotina do nó do proxy de montagem:
  - Especifique a opção managedservices com estes dois parâmetros:  
managedservices schedule webclient

Esta configuração direciona o client acceptor a gerenciar o Web client e o planejador.

- Se desejar direcionar informações de planejamento e de erro para arquivos de log diferentes dos arquivos padrão, especifique as opções schedlogname e errorlogname. Cada opção deve conter o caminho completo e o nome do arquivo no qual armazenar informações de log. Por exemplo:

```
schedlogname /vmsched/dsmsched_mp_lnx.log
errorlogname /vmsched/dsmerror_mp_lnx.log
```



- Para configurar o Client Acceptor Service e o Serviço do Planejador do Movedor de Dados para agir como um servidor de backup, configure a variável de ambiente a seguir no arquivo `/etc/init.d/dsmcad`:  

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```
- Inicie o Client Acceptor Service:  
O programa de instalação cria um script de inicialização para o client acceptor daemon (dsmcad) em `/etc/init.d`. O client acceptor daemon deve ser iniciado para que possa gerenciar as tarefas do planejador ou gerenciar o web client. Como raiz, use o comando a seguir para iniciar o daemon:  

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```

```
service dsmcad start
```

Para ativar o Client Acceptor Daemon para ser iniciado automaticamente após uma reinicialização do sistema, inclua o serviço conforme a seguir no prompt de shell:

```
# chkconfig --add dsmcad
```

6. Verifique se o aceitante do cliente e o agente estão configurados corretamente:
  - a. Efetue logon em um sistema remoto.
  - b. Use um navegador da web para se conectar ao sistema HOST1 usando este endereço e porta:  

```
http://HOST1.xyz.yourcompany.com:1581
```

---

## Configurando manualmente o nós do proxy de montagem em um sistema Windows remoto

### Windows

Conclua esta tarefa para incluir um nó do proxy de montagem em um sistema Windows remoto. Esta tarefa é necessária quando você deseja incluir um segundo nó do proxy de montagem Windows em seu ambiente.

### Antes de Iniciar

Antes de continuar com esta tarefa, certifique-se de que o nó do proxy de montagem do Windows primário esteja configurado.

### Sobre Esta Tarefa

Conclua estas etapas no sistema proxy de montagem do Windows remoto:

### Procedimento

1. Instale os produtos a seguir no sistema proxy de montagem do Windows remoto:
  - agente de recuperação
  - Movedor de dados do IBM Spectrum Protect

Acesse ambos os produtos na imagem de download do IBM Spectrum Protect for Virtual Environments. Instruções de instalação passo a passo estão disponíveis no IBM Knowledge Center em “Instalando os componentes do Proteção de Dados para VMware em sistemas Windows” na página 20

2. Recupere o conteúdo do arquivo de opções de amostra a partir do nó do proxy de montagem do Windows que foi criado e inclua-o no arquivo de opções no sistema proxy de montagem do Windows remoto:
  - a. No sistema proxy de montagem do Windows primário, acesse a janela Configuração no GUI do Data Protection for VMware vSphere.
  - b. Clique em **Editar Configuração do TSM** na lista de Tarefas. O bloco de notas de configuração pode levar alguns minutos para carregar.
  - c. Acesse a página Pares de Nós do Proxy de Montagem.
  - d. Na coluna Nó Primário da tabela, acesse o nó do proxy de montagem do Windows com o local pendente e clique em **Visualizar Configurações**.
  - e. Copie o conteúdo do arquivo dsm.opt de amostra que é mostrado no diálogo **Configurações de Proxy de Montagem**.
  - f. Cole (ou inclua) o conteúdo do arquivo dsm.opt de amostra no arquivo de opções no sistema proxy de montagem do Windows remoto. Nomeie o arquivo de opções com uma convenção que identifique sua função como um nó do proxy de montagem remoto.  
Por exemplo: dsm.REMOTE1\_MP\_WIN.opt.

**Restrição:** Não ative a opção sem a LAN (ENABLELANFREE YES) no arquivo de opções. Essa opção não é suportada para montagem de nós do proxy.

3. Emita este comando do movedor de dados para configurar o usuário e a senha do VMware vCenter para o nó do proxy de montagem:

**Dica:** Para iniciar a linha de comandos dsmsc, abra o menu **Iniciar do Windows** e selecione **Programas** → **IBM Spectrum Protect** → **Linha de Comandos do Cliente de Backup**.

```
dsmsc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
-optfile=dsm.REMOTE1_MP_WIN.opt
```

4. Verifique a conexão com o servidor IBM Spectrum Protect emitindo este comando:

```
dsmsc query session -optfile=dsm.REMOTE1_MP_WIN.opt
```

Este comando mostra informações sobre a sessão, incluindo o nome do nó atual, quando a sessão foi estabelecida, as informações do servidor e as informações de conexão do servidor.

5. Configure o Client Acceptor Service (CAD) e o Serviço do Planejador do Movedor de Dados concluindo estas etapas:

Esta etapa usa o assistente de Configuração da GUI do Cliente IBM Spectrum Protect para configurar o CAD e o Serviço do Planejador. Por padrão, o Serviço do Agente de Cliente Remoto também é configurado por meio do assistente. Se você usar o Utilitário de Configuração de Serviço do Cliente IBM Spectrum Protect (dsmscutil) para essa tarefa, certifique-se de instalar também o Serviço do Agente de Cliente Remoto.

Inicie o assistente de Configuração do Cliente IBM Spectrum Protect no menu de arquivo acessando **Utilitários** > **Assistente de Configuração**:

  - a. Selecione Ajude-me a configurar o TSM Web Client. Insira as informações conforme solicitado.
    - 1) Na opção Quando deseja que o serviço seja iniciado?, selecione Automaticamente quando o Windows for inicializado.

- 2) Na opção Gostaria de iniciar o serviço na conclusão deste assistente?, selecione Sim.

Quando a operação for concluída com êxito, retorne para a página de boas-vindas do assistente e prossiga para a Etapa b.

**Dica:** Ao configurar mais de um nó do proxy de montagem no mesmo sistema, você deve especificar um valor de porta diferente para cada instância do client acceptor.

- b. Selecione Ajude-me a Configurar o TSM Client Scheduler. Insira as informações conforme solicitado.
  - 1) Ao inserir o nome do planejador, certifique-se de selecionar a opção Usar o Client Acceptor Daemon (CAD) para gerenciar o planejador.
  - 2) Na opção Quando deseja que o serviço seja iniciado?, selecione Automaticamente quando o Windows for inicializado.
  - 3) Na opção Gostaria de iniciar o serviço na conclusão deste assistente?, selecione Sim.
6. Verifique se o client acceptor e o agente estão configurados corretamente. Use um navegador da web para se conectar ao sistema HOST1 usando este endereço e porta:  
`http://HOST1.xyz.yourcompany.com:1581`

---

## Configurando manualmente diversos serviços de client acceptor em um sistema Linux

Em determinadas circunstâncias, pode ser benéfico usar diversos serviços dsmcad em um único host do cliente Linux.

### Sobre Esta Tarefa

Esta tarefa configura diversas instâncias do dsmcad a serem executadas e iniciadas automaticamente no início do sistema:

### Procedimento

1. Crie duas sub-rotinas exclusivas do nó no arquivo dsm.sys (por padrão, esse arquivo está em /opt/tivoli/tsm/client/ba/bin/):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
COMMMethod          TCPip
TCPPort             1500
TCPServeraddress    localhost
nodename            node1
errorlogname         /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
schedlogname         /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
managedservices      webclient sched
httpport            1581
passwordaccess       generate

SErvername node2
COMMMethod          TCPip
TCPPort             1500
TCPServeraddress    localhost
nodename            node2
errorlogname         /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
schedlogname         /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
managedservices      webclient sched
httpport            1582
passwordaccess       generate
```

**Dica:** Pode ser útil incluir determinadas opções de inclusão/exclusão para diferenciar esses nós. Caso contrário, poderá ser feito o backup dos mesmos dados usando os dois nomes do nó.

2. Crie dois arquivos dsm.opt, um para cada nó (por padrão, esses arquivos estão em /opt/tivoli/tsm/client/ba/bin):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Ative passwordaccess generate efetuando login com as credenciais para ambos os nós:

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Faça duas cópias do script de inicialização rc.dsmcad padrão (por padrão, esse script está em /opt/tivoli/tsm/client/ba/bin):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Edite rc.dsmcad-node1:

- a. Mude esta linha para as distribuições do Red Hat Enterprise Linux:

```
daemon $DSMCAD_BIN
```

Para esta linha:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

- b. Mude esta linha para as distribuições do SUSE Linux Enterprise Server:

```
startproc $DSMCAD_BIN
```

Para esta linha:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

6. Edite rc.dsmcad-node2:

- a. Mude esta linha para as distribuições do Red Hat Enterprise Linux:

```
daemon $DSMCAD_BIN
```

Para esta linha:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

- b. Mude esta linha para as distribuições do SUSE Linux Enterprise Server:

```
startproc $DSMCAD_BIN
```

Para esta linha:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

7. Crie novos links em `/etc/init.d/` para apontar para os dois novos scripts de inicialização `rc.dsmcad`. Estes links permitem que o serviço de inicialização do Linux inicie os serviços `dsmcad` no início do sistema:

```
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
# ls -la dsm*
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

8. Registre os dois novos scripts `rc` com **chkconfig**:

```
# chkconfig --add dsmcad-node1
# chkconfig --add dsmcad-node2
```

9. Teste a configuração com o comando **service dsmcad start** para certificar-se de que os scripts sejam carregados e iniciados sem problema:

```
# service dsmcad-node1 start
Starting dsmcad-node1: [ OK ]
# service dsmcad-node2 start
Starting dsmcad-node2: [ OK ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

O texto de comando é colocado em duas linhas neste exemplo para acomodar a formatação da página.

10. Reinicie e confirme se as duas instâncias do `dsmcad` foram iniciadas automaticamente:

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

O texto de comando é colocado em duas linhas neste exemplo para acomodar a formatação da página.

---

## Modificando o Arquivo de Configuração VMCLI

O arquivo de configuração de VMCLI (`vmcliConfiguration.xml`) contém definições para o GUI do Data Protection for VMware vSphere.

O processo de instalação do Proteção de Dados para VMware requer que um usuário especifique um endereço IP do vCenter Server e se o acesso à GUI deve ser ativado pelo navegador da web. No entanto, após a instalação, o endereço IP do servidor e o método de acesso da GUI não podem ser modificados pelo instalador.

Para atualizar estas configurações, é possível editar manualmente o arquivo de configuração VMCLI (`vmcliConfiguration.xml`). Este arquivo é criado durante a instalação nos locais a seguir:

Nos sistemas Windows:

C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\tsmVmGUI

Nos sistemas Linux:

/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/

Para modificar deve-se ativar o acesso à GUI por um navegador da web, insira um dos valores a seguir no parâmetro **<enable\_direct\_start></enable\_direct\_start>**:

- *yes* A GUI pode ser acessada diretamente por um navegador da web. Por exemplo:

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* A GUI não pode ser acessada diretamente por um navegador da web. Por exemplo:

```
<enable_direct_start>no</enable_direct_start>
```

Para usar a GUI para proteção do vSphere, especifique o valor a seguir no parâmetro **<mode></mode>**:

- *vcenter* A GUI é usada para proteção do vSphere. Por exemplo:

```
<mode>vcenter</mode>
```

Para modificar o endereço IP do servidor vCenter, certifique-se de que **<mode>vcenter</mode>** esteja configurado, em seguida, especifique o endereço IP no parâmetro **<vcenter\_url></vcenter\_url>**. Por exemplo:

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

O valor `https://` é requerido no início do endereço IP do servidor vCenter. O valor `/sdk` é requerido no final do endereço IP do servidor vCenter.

## Arquivos `vmcliConfiguration.xml` de Exemplo

O arquivo `vmcliConfiguration.xml` a seguir está configurado para proteção de vSphere e o acesso do navegador da web está ativado para a GUI:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
  <VMCLIPath>C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts\
</VMCLIPath>
  <interruptDelay>900000</interruptDelay>
  <mode>vcenter</mode>
  <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
  <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

---

## Apêndice B. Migrando para uma estratégia de backup incremental contínuo

Use este procedimento para migrar planejamentos de backup existentes, políticas e nó do movedor de dados para uso em uma estratégia de backup incremental contínuo.

### Antes de Iniciar

É possível usar a estratégia de backup completo incremental contínuo que foi implementada no Proteção de Dados para VMware versão 6.2 e 6.3. Se você deseja continuar a usar a estratégia de backup completo incremental contínuo, não será necessário mudar sua política ou planejamentos. Você deve certificar-se de fazer upgrade apenas dos nós do movedor de dados para a versão 6.4 (ou mais recente), conforme documentado no procedimento a seguir. No entanto, se você deseja usar a estratégia de backup incremental contínuo, além de atualizar os nós do movedor de dados para a versão 6.4 (ou posterior), deve-se também atualizar os planejamentos e política para os nós do movedor de dados que se movem para essa estratégia de backup incremental contínuo.

Para migrar planejamentos existentes do Proteção de Dados para VMware para uma estratégia de backup incremental contínuo, deve-se concluir as tarefas documentadas neste procedimento.

### Importante:

- Embora algumas tarefas sejam discretas, todos os aplicativos e componentes devem ter upgrade efetuado eventualmente para se beneficiarem completamente da estratégia incremental contínuo. Esta publicação fornece todas as informações que orientam você em cada tarefa.
- Há diversos métodos disponíveis para executar o processo de migração inteiro. Entretanto, os métodos documentados nesta publicação são considerados eficientes para ambientes típicos do Proteção de Dados para VMware.
- O planejamento a ser migrado nesse procedimento é um que foi criado com o assistente de backup do GUI do Data Protection for VMware vSphere. Se o planejamento a ser migrado foi criado manualmente, as atualizações de planejamento identificadas nesse procedimento também deverão ser feitas manualmente.

### Sobre Esta Tarefa

#### Procedimento

1. Atualize todos os Servidores de Backup vStorage que protegem um único vCenter. Certifique-se de que esse upgrade seja concluído no mesmo horário para todos os nós do movedor de dados.
  - Este upgrade requer a instalação do Movedor de Dados do IBM Spectrum Protect versão 6.4 (ou mais recente) no Servidor de Backup vStorage.
  - Como uma tarefa discreta, você não precisa executar a Etapa 2 ou 3 imediatamente após a Etapa 1. Após o upgrade dos nós do movedor de dados, é possível continuar fazendo backup das MVs em seu ambiente existente. Execute a Etapa 2 e 3 quando uma oportunidade mais conveniente se tornar disponível.

**Dica:** Se o seu ambiente usar diversos Servidores de Backup vStorage, considere atualizar apenas um servidor. Em seguida, verifique se o servidor opera com êxito antes de atualizar o restante dos Servidores de Backup vStorage.

2. Atualize a política de backup e os planejamentos de backup para implementar backups incrementais contínuos:

Execute as tarefas de política de backup a seguir no servidor IBM Spectrum Protect emitindo comandos no cliente da linha de comandos administrativa (dsmadm):

- a. Crie uma classe de gerenciamento para o domínio apropriado e o conjunto de políticas para seus backups incrementais contínuos. Esse exemplo cria a classe de gerenciamento `mgmt_ifincr28` para o domínio `domain1` e o conjunto de política `prodbackups`. O nome da classe de gerenciamento é usado para descrever uma estratégia de backup incremental contínuo que retém 28 versões de backup:

```
define mgmtclass domain1 prodbackups mgmt_ifincr28
description="Reten 28 versões de backup"
```

- b. Crie um grupo de cópias de backup para seus backups incrementais contínuos. Esse exemplo cria um grupo de cópias de backup padrão para o domínio `domain1`, o conjunto de políticas `prodbackups` e a classe de gerenciamento `mgmt_ifincr28`:

```
define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
```

As entradas `standard type=backup` são valores padrão e não precisam ser especificadas. Elas foram incluídas nesse exemplo para ilustrar que o nome do grupo de cópias é `STANDARD` e que o tipo de grupo de cópias é `backup` (em vez de `archive`).

- c. Atualize o grupo de cópias de backup com as configurações apropriadas de versão, retenção e expiração:

**Lembre-se:** No Proteção de Dados para VMware versão 6.2 e 6.3, a versão de backup, retenção e expiração são baseadas em um nível de granularidade de cadeia de backups. Esse método significa que embora os backups completos incrementais contínuos e incrementais contínuos sejam feitos (como parte da estratégia de backup completo incremental contínuo 6.2 e 6.3), a expiração de versão conta apenas backups completos. No Proteção de Dados para VMware versão 6.4 (ou mais recente), a versão de backup, retenção e expiração são baseadas em um nível de granularidade de backup único. Esse método significa que a expiração de versão conta os backups completos incrementais contínuos e incrementais contínuos.

O parâmetro `verexists` especifica o número máximo de versões de backup da MV no servidor. Se uma operação de backup incremental contínuo exceder o número, o servidor expirará a versão de backup mais antiga existente no armazenamento do servidor. Esse exemplo especifica `verexists=28`. Esse valor significa que no máximo 28 versões de backup da MV são retidos no servidor.

O parâmetro `retextra` especifica o número máximo de dias para reter uma versão de backup da MV, após essa versão tornar-se inativa. Esse exemplo especifica `retextra=no limit`. Esse valor significa que o número máximo de versões inativas de backup da MV é retido indefinidamente. Entretanto, quando `verexists` é especificado, o valor `no limit` é substituído pelo valor `verexists`. Como resultado, nesse exemplo, um número máximo de 28 versões inativas de backup da MV é retido no servidor.



Com base nas configurações descritas nesta etapa, o grupo de cópias de backup é atualizado da seguinte forma:

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28  
retextra=nolimit
```

Nesse exemplo, o ambiente existente do Proteção de Dados para VMware versão 6.3 consiste nos seguintes hosts e planejamentos:

- Um cluster ESX (esxcluster) que contém dois hosts ESX (esxhost1, esxhost2).
- O planejamento bup\_esxcluster\_full executa um backup completo incremental contínuo semanalmente de cada host ESX com o nó do movedor de dados dm1.
- O planejamento bup\_esxcluster\_incr executa um backup incremental contínuo diário de cada host ESX com o nó do movedor de dados dm2.

Execute as tarefas de planejamento de backup a seguir no GUI do Data Protection for VMware vSphere:

- a. Inicie o GUI do Data Protection for VMware vSphere clicando no ícone na janela Soluções e Aplicativos do vSphere Client.
  - b. Na janela Introdução, clique na guia **Backup** para abrir a janela Gerenciando planejamentos de backup.
  - c. Localize o planejamento de backup (usado para backups completos incrementais contínuos ou incrementais) para atualizar. Neste procedimento, o planejamento completo incremental contínuo bup\_esxcluster\_full é usado.
  - d. Clique com o botão direito no planejamento e selecione **Propriedades**.
  - e. Acesse a página Planejamento e especifique **Incremental** na lista suspensa **Estratégia de backup**.
  - f. Clique em **OK** para salvar a atualização.
  - g. Localize o planejamento de backup usado para backups incrementais contínuos. Clique com o botão direito no planejamento e selecione **Excluir**. Como o planejamento completo incremental contínuo bup\_esxcluster\_full foi atualizado para incremental contínuo, esse planejamento incremental contínuo não é mais necessário.
3. Agora que você tem um planejamento de backup incremental contínuo, será possível reduzir o número de nós do movedor de dados consolidando-os: Este exemplo consolida dois nós do movedor de dados em apenas um.
- a. No Servidor de Backup vStorage, abra um prompt de comandos e acesse o diretório no qual o arquivo de opções para dm1 está localizado.
  - b. Usando um editor de texto (como o Notepad), atualize esse arquivo com as opções a seguir:
    - 1) Especifique `vmmaxparallel` para controlar o número de MVs cujo backup é feito de uma vez por dm1:  
`vmmaxparallel=2`

O valor padrão e o valor mínimo são 1. O valor máximo é 50.

**Dica:** Para cada nó do movedor de dados removido, aumente o valor `vmmaxparallel` em 1.

Como alternativa, é possível especificar `vmlimitsperhost` para controlar o número de MVs com backup feito de uma vez por dm1 do mesmo host ESX:

```
vm limitperhost=1
```

Essa opção é útil ao desejar impedir que um host fique sobrecarregado. O valor padrão é 0 (sem limite). O valor mínimo é 1. O valor máximo é 50.

- c. Efetue logon no servidor IBM Spectrum Protect. Use o cliente da linha de comandos administrativa (dsmadm) para especificar o número máximo de sessões simultâneas de backup da MV que pode conectar-se ao servidor. Por exemplo:  

```
maxsessions=4
```

O valor padrão é 25. O valor mínimo é 2.

- 4. Verifique se os nós do movedor de dados atualizados estão funcionando corretamente:
  - a. Inicie o GUI do Data Protection for VMware vSphere clicando no ícone da janela Soluções e Aplicativos do vSphere Client.
  - b. Na janela Introdução, clique na guia Configuração para visualizar a página Status de Configuração.
  - c. Na página Status de Configuração, selecione o vCenter que foi protegido na Etapa 1. Clique em um nó do movedor de dados para visualizar suas informações de status na área de janela Detalhes do Status. Quando um nó exibir um aviso ou um erro, clique nele e use as informações na área de janela Detalhes de Status para resolver o problema. Em seguida, selecione o nó e clique em **Validar Nó Selecionado** para verificar se o problema é resolvido. Clique em Atualizar para testar novamente todos os nós.

## Resultados

Na conclusão bem-sucedida de cada tarefa, o ambiente está pronto para uso em uma estratégia de backup incremental contínuo.

**Restrições:** após a migração dos planejamentos de tipos de backups completos incrementais contínuos para tipos de backups incrementais contínuos, esteja ciente das restrições a seguir:

- Mudar planejamentos migrados de volta para tipos de backups completos incrementais contínuos por VM (máquina virtual) (espaço no arquivo) não é suportado.
- Usar uma versão anterior do movedor de dados do IBM Spectrum Protect em um espaço no arquivo migrado não é suportado.
- Quando um espaço no arquivo contém um (ou mais) backups incrementais contínuos, um backup completo incremental contínuo não é suportado.

## Exemplo de controle de versão com o parâmetro verexists

Nesse exemplo de migração de planejamento, o Proteção de Dados para VMware versão 6.3 usa os dois planejamentos de backup a seguir:

- `-mode=full`: um backup completo incremental contínuo semanal é planejado (domingos) e o número máximo de versões de backup da VM (máquina virtual) a ser retido no servidor é quatro (`verexists=4`).
- `-mode=incr`: um backup incremental contínuo em dia de semana é planejado (segunda a sábado).

O número de backups feito em um período de quatro semanas é 28:

- Quatro backups completos incrementais contínuos (um backup completo semanal multiplicado por quatro semanas)
- 24 backups incrementais contínuos (seis backups incrementais em dia de semana multiplicados por quatro semanas)

Como o Proteção de Dados para VMware versão 6.3 conta apenas backups completos, o valor `verexists=4` preserva os 28 backups.

Para fornecer o mesmo nível de proteção com o Proteção de Dados para VMware versão 6.4 (ou posterior) e a estratégia de backup incremental contínuo, crie o planejamento a seguir:

`-mode=iffull`: um backup completo incremental contínuo diário é planejado e o parâmetro `verexists` é configurado para 28.

O número de backups feito em um período de quatro semanas é 28:

- Um backup completo incremental contínuo (backup inicial multiplicado por um dia)
- 27 backups incrementais contínuos (backups incrementais contínuos diários multiplicados por 27 dias)

Como o Proteção de Dados para VMware versão 6.4 (ou posterior) conta os backups completos incrementais contínuos e incrementais contínuos, o valor de `verexists=28` preserva todos os 28 backups.



---

## Apêndice C. Recursos de Acessibilidade para a Família de Produtos IBM Spectrum Protect

Os recursos de acessibilidade ajudam os usuários que possuem uma deficiência, como mobilidade restrita ou visão limitada, a usar o conteúdo de tecnologia da informação com êxito.

### Visão Geral

A família de produtos IBM Spectrum Protect inclui os principais recursos de acessibilidade a seguir:

- Operação apenas do teclado
- Operações que usam um leitor de tela

A família de produtos IBM Spectrum Protect usa o padrão W3C mais recente, WAI-ARIA 1.0 ([www.w3.org/TR/wai-aria/](http://www.w3.org/TR/wai-aria/)), para assegurar conformidade com o US Section 508 ([www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards)) e Web Content Accessibility Guidelines (WCAG) 2.0 ([www.w3.org/TR/WCAG20/](http://www.w3.org/TR/WCAG20/)). Para aproveitar os recursos de acessibilidade, use a liberação mais recente do seu leitor de tela e o último navegador da web que seja suportado pelo produto.

A documentação do produto no IBM Knowledge Center é ativada para acessibilidade. Os recursos de acessibilidade do IBM Knowledge Center estão descritos na seção de Acessibilidade da ajuda do IBM Knowledge Center ([www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility](http://www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility)).

### Navegação pelo Teclado

Esse produto usa as chaves de navegação padrão

### Informações sobre a Interface

As interfaces com o usuário não têm conteúdo que pisca 2-55 vezes por segundo.

Interfaces com o usuário da web dependem de folhas de estilo em cascata para renderizar o conteúdo corretamente e para fornecer uma experiência utilizável. O aplicativo fornece uma maneira equivalente para os usuários com visão reduzida usarem as configurações de exibição do sistema, incluindo o modo de alto contraste. É possível controlar o tamanho da fonte usando as configurações do dispositivo ou do navegador da web.

As interfaces com o usuário da web incluem referências de navegação WAI-ARIA que podem ser usadas para navegar rapidamente para áreas funcionais no aplicativo.

### Software do Fornecedor

A família de produtos do IBM Spectrum Protect inclui determinado software de fornecedor que não é coberto pelo contrato de licença da IBM. A IBM não representa nenhum recurso de acessibilidade desses produtos. Entre em contato

com o fornecedor para obter informações de acessibilidade sobre estes produtos.

### **Informações sobre acessibilidade relacionadas**

Além dos websites padrão do IBM help desk e do suporte, a IBM tem um serviço telefônico TTY para ser usado por clientes com deficiência auditiva para acessar os serviços de suporte e vendas:

Serviço de TTY  
800-IBM-3383 (800-426-3383)  
(na América do Norte)

Para obter informações adicionais sobre o compromisso que a IBM tem com a acessibilidade, consulte Acessibilidade IBM([www.ibm.com/able](http://www.ibm.com/able)).

---

## Aviso

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. Este material pode estar disponível na IBM em outros idiomas. No entanto, pode ser necessário possuir uma cópia do produto ou da versão de produto no mesmo idioma para acessá-lo.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

*Gerência de Relações Comerciais e Industriais da IBM Brasil*  
*Av. Pasteur, 138-146*  
*Botafogo*  
*Rio de Janeiro, RJ*  
*CEP 22290-240*

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

*Intellectual Property Licensing*  
*Legal and Intellectual Property Law*  
*IBM Japan Ltd.*  
*19-21, Nihonbashi-Hakozakicho, Chuo-ku*  
*Tokyo 103-8510, Japan*

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO-INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Esta publicação pode conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode fazer aperfeiçoamentos e/ou alterações nos produtos ou programas descritos nesta publicação a qualquer momento sem aviso prévio.

As referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, devem entrar em contato com:

*Gerência de Relações Comerciais e Industriais da IBM Brasil*  
*Av. Pasteur, 138-146*  
*Botafogo*  
*Rio de Janeiro, RJ*  
*CEP 22290-240*

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer outro contrato equivalente entre as partes.

Os dados de desempenho discutidos aqui são apresentados como derivados sob as condições de operação específicas. Os resultados reais poderão variar.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas aos fornecedores desses produtos.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

#### LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem



garantia de qualquer tipo. A IBM não poderá ser responsabilizada por quaisquer danos decorrentes ao uso dos programas de amostra.

Qualquer cópia, parte desses programas de amostra ou trabalho derivado deve incluir um aviso de copyright da seguinte forma: © (o nome de sua empresa) (ano). Partes deste código são derivadas dos Programas de Amostra da IBM Corp. © Copyright IBM Corp. \_insira o ano ou anos\_.

## **Marcas**

IBM, o logotipo IBM e ibm.com são marcas registradas ou comerciais da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas comerciais IBM está disponível na web em "Copyright and trademark information" em [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe é uma marca registrada da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Linear Tape-Open, LTO e Ultrium são marcas comerciais da HP, IBM Corp. e Quantum nos Estados Unidos e em outros países.

Intel e Itanium são marcas comerciais ou marcas registradas da Intel Corporation ou de suas subsidiárias nos Estados Unidos e em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows e Windows NT são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

SoftLayer é uma marca registrada da SoftLayer, Inc., uma empresa IBM.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

## **Termos e Condições para a Documentação do Produto**

As permissões para uso dessas publicações são concedidas sujeitas aos termos e condições a seguir.

### **Aplicabilidade**

Esses termos e condições são adicionais a quaisquer termos de uso para o website da IBM.

### **utilizar o Personal**

Você pode reproduzir estas publicações para seu uso pessoal não comercial desde que todos os avisos do proprietário sejam preservados. O Cliente não pode distribuir, exibir ou fazer trabalho derivado destas publicações, ou de parte delas, sem o consentimento expresso da IBM.

### **Uso comercial**

É possível reproduzir, distribuir e exibir estas publicações exclusivamente

dentro de sua empresa desde que todos os avisos do proprietário sejam preservados. O Cliente não pode fazer trabalhos derivados destas publicações ou reproduzir, distribuir ou exibir estas publicações, ou qualquer parte delas, fora de sua empresa, sem o consentimento expresso da IBM.

#### **Direitos**

Exceto como expressamente concedido nesta permissão, nenhuma outra permissão, licença ou direito é concedido, seja expresso ou implícito, para as publicações ou para quaisquer informações, dados, software ou outra propriedade intelectual nelas contidos.

A IBM reserva-se o direito de retirar as permissões concedidas aqui sempre que, a seu critério, o uso das publicações prejudicar seus interesses ou, conforme determinação da IBM, as instruções anteriores não estão sendo seguidas adequadamente.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto em conformidade total com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação dos Estados Unidos.

A IBM NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

#### **Considerações sobre política de privacidade**

Os produtos de Software IBM, incluindo as soluções de software como serviço ("Ofertas de Software"), podem usar cookies ou outras tecnologias para coletar informações sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem permitir a coleta de informações identificáveis pessoalmente. Se esta Oferta de Software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão apresentadas abaixo.

Esta Oferta de Software não usa cookies ou outras tecnologias para coletar informações pessoalmente identificáveis.

Se as configurações implementadas para esta Oferta de software fornecerem a você, como cliente, a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, é necessário buscar seu próprio conselho jurídico legal sobre quaisquer leis aplicáveis a este tipo de coleção de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter informações adicionais sobre o uso de várias tecnologias, incluindo cookies, para estes propósitos, consulte a Política de privacidade da IBM em <http://www.ibm.com/privacy> e a Declaração de privacidade on-line da IBM em <http://www.ibm.com/privacy/details> na seção intitulada "Cookies, Web Beacons and Other Technologies" e "IBM Software Products and Software-as-a-Service Privacy Statement" em <http://www.ibm.com/software/info/product-privacy>.

---

## **Glossário**

Está disponível um glossário com termos e definições para a família de produtos IBM Spectrum Protect.

Consulte o IBM Spectrum Protectglossário.

Para visualizar glossários para outros produtos IBM, consulte IBM Terminology.



---

# Índice Remissivo

## A

- aceitante do cliente
  - configurando 105
- acesso ao keystore
  - certificado de terceiro 56
- agente de recuperação 6
- armazenamento em fita
  - configurando 94
- arquivo de configuração VMCLI
  - modificando 107
  - vmcliConfiguration.xml 107
- assistente de configuração 41
- assistente de instalação
  - Linux
    - usando o assistente de instalação 22
  - Windows
    - usando o assistente de instalação 20
- atualizando
  - a partir da V6.x
    - padrão 32
  - Linux
    - silenciosa 34
  - visão geral 32
  - Windows de 64 bits
    - silenciosa 33
- autoridade
  - permissões 12

## B

- bloco de notas da configuração 42

## C

- certificado de terceiro
  - acesso ao keystore 56
  - configurando TLS 55
  - criar um certificate signing request 57
  - enviar o certificate signing request 58
  - receber o certificado assinado 58
- chave de registro 18, 67
- código de idioma
  - configurações 77
- componentes 1
  - agente de recuperação 6
  - componentes instaláveis 19
  - Extensão do IBM Spectrum Protect 7
  - GUI de restauração do arquivo 8
  - GUI do Data Protection for VMware vSphere 3
  - Interface da linha de comandos do Data Protection for VMware 7
  - movimentador de dados 8
- componentes instaláveis 1
  - agente de recuperação 6
  - Extensão do IBM Spectrum Protect 7
  - GUI de restauração do arquivo 8
  - GUI do Data Protection for VMware vSphere 3
  - Interface da linha de comandos do Data Protection for VMware 7
  - movimentador de dados 8

- comunicação TLS
  - configurando 55
- configurando
  - aceitante do cliente 105
  - ambiente do vSphere
    - lista de verificação da linha de comandos 91
  - armazenamento em fita 94
  - arquivo de configuração VMCLI 107
  - comunicação do navegador da web 55
  - comunicação TLS 55
  - configuração existente 42
  - configuração inicial 41
  - configurações do código de idioma 77
  - GUI do agente de recuperação 68
  - montagem de iSCSI 96, 99
  - Nós do IBM Spectrum Protect
    - ambiente do vSphere 82
  - nós do movedor de dados
    - ambiente do vSphere 83
  - nós do proxy de montagem
    - Linux 101
    - Windows 103
  - planilha para o Proteção de Dados para VMware 30
  - SSL 55
  - tarefas avançadas 81
  - visão geral 41
  - VMCLI
    - ambiente do vSphere 88
- configurando TLS
  - autoridade de certificação 55
  - certificado de terceiro 55
  - permitir comunicação segura com o servidor 60, 73, 74, 75
- configurar
  - restauração de arquivo
    - opções 45
- configurar o
  - ativar restauração de arquivo 43
  - ativar suporte de identificação 49
- credenciais
  - permissões 12
- criar um certificate signing request
  - certificado de terceiro 57

## D

- deficiência 115
- desinstalação silenciosa
  - Linux
    - modo silencioso 38
  - Windows de 64 bits
    - modo silencioso 37
- desinstalando
  - Linux
    - modo silencioso 38
    - típico 35
  - Windows de 64 bits
    - modo silencioso 37
    - típico 35

## E

- enviar o certificate signing request
  - certificado de terceiro 58
- Extensão do IBM Spectrum Protect 7

## G

- GUI
  - GUI do Data Protection for VMware vSphere 31
- GUI de restauração do arquivo 8
- GUI do agente de recuperação
  - configurando 68
  - opções 68
- GUI do Data Protection for VMware vSphere 3, 31
  - permissões
  - operações 64
- GUI do vSphere 31

## I

- IBM Knowledge Center v
- instalação
  - componentes 19
- instalação silenciosa
  - Linux 27
  - Windows de 64 bits
    - instalador Suite silencioso 24
- instalando
  - componentes instaláveis 1
  - fazendo download do pacote 19
  - Linux
    - usando o assistente de instalação 22
  - obtendo o pacote 19
  - permissões do usuário 12
  - portas de comunicação necessárias 13
  - Proteção de Dados para VMware 1
  - requisitos de hardware 11
  - requisitos de software 11
  - requisitos do sistema 11
  - roteiro 9
  - Windows
    - usando o assistente de instalação 20
- Interface da linha de comandos do Data Protection for VMware 7

## K

- Knowledge Center v

## L

- Linux
  - atualizando
    - silenciosa 34
  - desinstalando
    - modo silencioso 38
    - típico 35
  - procedimento de instalação
    - limpa 22
    - silenciosa 27
- logging
  - restauração de arquivo 47

## M

- migrando
  - planejamentos 109
- montagem de iSCSI
  - configurando 96, 99
- movimentador de dados 8
  - nós
    - configurando no ambiente do vSphere 83

## N

- Nós do IBM Spectrum Protect
  - configurando
    - ambiente do vSphere 82
- Novo no Data Protection for VMware Versão 7.1.6 vii

## P

- permissões
  - GUI do Data Protection for VMware vSphere
    - operações 64
    - instalação 12
- permitir comunicação segura com o servidor
  - configurando TLS 60, 73, 74, 75
- planejamento
  - requisitos do sistema 11
- planejando
  - permissões 12
  - portas de comunicação necessárias 13
  - roteiro 9
  - visão geral 9
- portas
  - instalação 13
- portas de comunicação
  - instalação 13
- privilegio de administrador
  - GUI do Data Protection for VMware vSphere 64
- procedimento de instalação
  - Linux
    - limpa 22
    - silenciosa 27
  - Windows de 64 bits
    - instalador Suite silencioso 24
- Proteção de Dados para VMware
  - componentes instaláveis 1
  - fazendo download do pacote 19
  - planejando 9
- publicações v

## R

- receber o certificado assinado
  - certificado de terceiro 58
- recursos de acessibilidade 115
- requisitos de hardware 11
- requisitos de software 11
- requisitos do sistema 11
- restauração
  - agente de recuperação 6
- restauração de arquivo
  - ambiente Linux 44
  - ativar 43
  - configurando a criação de log 47
  - configurando opções 45
  - opções 46, 48

- restaurar
  - arquivo 45, 46, 47, 48
  - configurando a criação de log 47
  - configurando opções 45
  - opções 46, 48

## S

- serviços 80
- SSL
  - configurando 55, 60, 73, 74, 75
- suporte de identificação
  - ativar 49

## T

- teclado 115

## U

- upgrade silencioso
  - Linux 34
  - Windows de 64 bits 33
- usuário
  - permissões 12

## V

- VMCLI
  - configurando no ambiente do vSphere 88

## W

- Windows de 64 bits
  - atualizando
    - silenciosa 33
  - desinstalando
    - modo silencioso 37
    - típico 35
  - procedimento de instalação
    - instalador Suite silencioso 24









Número do Programa: 5725-X00

Impresso no Brasil