

IBM Spectrum Protect Plus
Versão 10.1.4

Guia do usuário e de instalação



Nota:

Antes de usar estas informações e o produto suportado por elas, leia as informações em [“Avisos” na página 319](#).

Esta edição se aplica à versão 10, liberação 1, modificação 4 do IBM Spectrum Protect Plus (número do produto 5737-F11) e a todas as liberações e modificações subsequentes, até que seja indicado de outra forma em novas edições.

© **Copyright International Business Machines Corporation 2017, 2019.**

Índice

Sobre esta publicação.....	vii
Quem Deve Ler essa Publicação.....	vii
Publicações	vii
O Que Há de Novo em Versão 10.1.4	ix
Envolvendo-se no desenvolvimento do produto.....	xi
Programa do usuário patrocinador.....	xi
Programa beta.....	xi
Capítulo 1. Visão geral do produto.....	1
Componentes do Produto.....	1
Painel do Produto.....	3
Alertas.....	4
Controle de Acesso Baseado na Função.....	5
Replicar dados de armazenamento de backup.....	5
Transfload para armazenamento de backup secundário.....	6
IBM Spectrum Protect Plus no IBM Cloud.....	9
IBM Spectrum Protect Plus no AWS.....	10
Capítulo 2. Instalando o IBM Spectrum Protect Plus.....	11
Roteiro de implementação do produto.....	11
Requisitos de Sistema	11
Requisitos do Componente	11
Requisitos do Hypervisor	23
Requisitos de Indexação de Arquivo e Restauração.....	24
Requisitos do Microsoft Exchange Server.....	28
Requisitos do Db2.....	31
Requisitos do MongoDB.....	34
Requisitos do Oracle.....	37
Requisitos do Microsoft SQL Server.....	41
Obtendo o pacote de instalação do IBM Spectrum Protect Plus.....	45
Instalando o IBM Spectrum Protect Plus como um dispositivo virtual VMware.....	46
Instalando o IBM Spectrum Protect Plus como um dispositivo virtual Hyper-V.....	48
Designando um endereço IP estático.....	50
Fazendo Upload da Chave do Produto.....	50
Editando portas de firewall.....	51
Capítulo 3. Instalando e configurando servidores vSnap.....	53
Instalando servidores vSnap.....	53
Instalando um servidor vSnap físico.....	53
Instalando um servidor vSnap virtual em um ambiente VMware.....	54
Instalando um servidor vSnap virtual em um ambiente Hyper-V.....	55
Gerenciando servidores vSnap.....	56
Incluindo um servidor vSnap como um provedor de armazenamento de backup.....	56
Inicializando o servidor vSnap.....	58
Configurando opções de armazenamento vSnap.....	59
Expandindo um conjunto de armazenamentos vSnap.....	60
Estabelecendo uma parceria de replicação para servidores vSnap.....	60
Alterando a taxa de rendimento de transferência de transferência.....	61

Referência de administração do servidor vSnap	62
Gerenciamento de armazenamento.....	63
Gerenciamento de rede.....	66
Desinstalando um servidor vSnap.....	66
Capítulo 4. Desiniciando para um Início Rápido.....	69
Inicie o IBM Spectrum Protect Plus.....	71
Gerenciar sites.....	72
Criar políticas de backup.....	73
Criar uma conta do usuário para o administrador do aplicativo.....	74
Incluir recursos para proteger.....	76
Incluir recursos em uma definição de tarefa.....	78
Inicie a tarefa de backup.....	79
Executar um relatório.....	80
Capítulo 5. Atualizando componentes do IBM Spectrum Protect Plus.....	83
Atualizando o dispositivo virtual IBM Spectrum Protect Plus.....	83
Atualizando servidores vSnap.....	85
Atualizando o sistema operacional para um servidor vSnap físico.....	85
Atualizando o sistema operacional para um servidor vSnap virtual.....	86
Atualizando um servidor vSnap.....	86
Atualizando proxies VADP.....	87
Aplicando atualizações de disponibilidade antecipada.....	88
Capítulo 6. Gerenciar políticas SLA para operações de backup.....	89
Criando uma política de SLA.....	89
Editando uma política de SLA.....	93
Excluindo uma política de SLA.....	93
Capítulo 7. Protegendo hypervisors.....	95
VMware.....	95
Incluindo uma Instância do vCenter Server.....	95
Fazendo backup dos dados de VMware.....	103
Gerenciando proxies de backup do VADP.....	107
Restaurando Dados do VMware.....	111
Hyper-V.....	121
Incluindo um servidor Hyper-V.....	121
Fazendo Backup de Dados do Hyper-V.....	124
Restaurando dados do Hyper-V.....	127
Restaurando arquivos.....	133
Capítulo 8. Protegendo Aplicativos.....	137
Db2.....	137
Pré-requisitos para o Db2.....	137
Incluindo um servidor de aplicativos Db2.....	141
Fazendo backup de dados do Db2.....	144
Restaurando Dados do Db2	151
Exchange Server.....	161
Pré-requisitos.....	161
Privilégios	161
Incluindo um servidor de aplicativos do Exchange.....	163
Fazendo backup de bancos de dados Microsoft Exchange	164
Estratégia de Backup Incremental Contínuo.....	167
Restaurando Microsoft Exchange bancos de dados	168
Acessando arquivos de banco de dados do Exchange com o modo de acesso instantâneo.....	194
MongoDB.....	196
Pré-requisitos para o MongoDB.....	197

Incluindo um servidor de aplicativos MongoDB.....	199
Fazendo backup de dados do MongoDB.....	203
Restaurando Dados do MongoDB	208
SQL Server.....	222
Incluindo um servidor de aplicativos SQL Server.....	223
Fazendo Backup dos Dados do SQL Server.....	225
Restaurando os Dados do SQL Server.....	228
Oracle.....	235
Incluindo um servidor de aplicativos Oracle.....	235
Fazendo Backup de Dados do Oracle.....	237
Restaurando dados do Oracle.....	240
Capítulo 9. Protegendo IBM Spectrum Protect Plus.....	247
Fazendo Backup do Aplicativo.....	247
Restaurando o aplicativo.....	247
Gerenciando pontos de restauração.....	248
Excluindo recursos do IBM Spectrum Protect Plus do catálogo.....	249
Capítulo 10. Tarefas e operações.....	251
Tipos de Tarefa.....	251
Iniciando Tarefas.....	252
Pausando e Continuando Tarefas.....	253
Cancelando Tarefas.....	253
Executando novamente as tarefas de backup parcialmente concluídas.....	253
Fazendo Backup de um Recurso Único.....	254
Configurando scripts para operações de backup e restauração.....	255
Fazendo Upload de um Script.....	255
Incluindo um script em um servidor.....	255
Capítulo 11. Configurando e Mantendo o Ambiente do Sistema IBM Spectrum Protect Plus.....	257
Gerenciando o armazenamento de backup secundário.....	257
Gerenciando o armazenamento em.....	257
Gerenciando o armazenamento do servidor de.....	262
Gerenciando Chaves e Certificados.....	268
Gerenciando sites.....	271
Incluindo um Site.....	271
Editando um Site.....	272
Excluindo um Site.....	273
Gerenciando servidores LDAP e SMTP.....	274
Incluindo um servidor LDAP.....	274
Incluindo um servidor SMTP.....	275
Editando configurações para um servidor LDAP ou SMTP.....	276
Excluindo um servidor LDAP ou SMTP.....	277
Aplicando preferências globais.....	277
Efetuando Logon no Console Administrativo.....	278
Configurando o fuso horário.....	279
Fazendo upload de um certificado SSL a partir do console administrativo.....	280
Fazendo upload de um certificado SSL a partir da linha de comandos.....	281
Efetuando logon no dispositivo virtual.....	281
Acessando o dispositivo virtual no VMware.....	281
Acessando o dispositivo virtual no Hyper-V.....	282
Testando a conectividade de rede.....	282
Executando a Ferramenta de Serviço a partir de uma interface da linha de comandos.....	282
Executando a Ferramenta de Serviço remotamente.....	283
Incluindo discos virtuais.....	284
Incluindo um disco no dispositivo virtual.....	284

Incluindo capacidade de armazenamento de um novo disco para o volume do dispositivo.....	285
Capítulo 12. Gerenciando relatórios e logs.....	289
Tipos de relatório.....	289
Relatórios de Utilização de Armazenamento de Backup.....	289
Relatórios de proteção.....	290
Relatórios do sistema.....	291
Relatórios de Ambiente da VM.....	292
Relatar Ações.....	293
Executando um relatório.....	294
Criando um Relatório Customizado.....	294
Planejando um relatório.....	294
Coletando e revisando logs de auditoria para ações.....	295
Capítulo 13. Gerenciando o acesso de.....	297
Gerenciando grupos de recursos do usuário.....	297
Criando um Grupo de Recursos.....	297
Editando um Grupo de Recursos.....	300
Excluindo um Grupo de Recursos.....	301
Gerenciando atribuições.....	301
Criando uma função.....	302
Editando uma função.....	305
Excluindo uma função.....	305
Gerenciando contas do usuário.....	305
Criando uma conta do usuário para um usuário individual.....	305
Criando uma conta do usuário para um grupo LDAP.....	306
Editando Credenciais de Conta do Usuário.....	307
Excluindo uma Conta do Usuário.....	307
Gerenciando identidades.....	307
Incluindo uma Identidade.....	307
Editando uma Identidade.....	308
Excluindo uma Identidade.....	308
Capítulo 14. Visão geral do licenciamento.....	309
Tags do Software License Metric (SLM).....	309
Integração com o IBM License Metric Tool (ILMT).....	310
Capítulo 15. Detecção de problemas.....	311
Coletando Arquivos de Log para Resolução de Problemas.....	311
Capítulo 16. Mensagens do produto.....	313
Prefixos de mensagem.....	313
Apêndice A. Diretrizes de Procura.....	315
Apêndice B. Acessibilidade.....	317
Avisos.....	319
Glossário.....	323
Índice Remissivo.....	325

Sobre esta publicação

Esta publicação fornece instruções de visão geral, de planejamento, de instalação e de usuário para o IBM Spectrum Protect Plus.

Quem Deve Ler essa Publicação

Esta publicação destina-se a administradores e usuários que são responsáveis pela implementação de uma solução de backup e recuperação com o IBM Spectrum Protect Plus em um dos ambientes suportados.

Nesta publicação, supõe-se que você tem um entendimento dos aplicativos que suportam o IBM Spectrum Protect Plus, conforme descrito em [“Requisitos de Sistema”](#) na página 11.

Publicações

A família de produtos do IBM Spectrum Protect inclui IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, 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 em Versão 10.1.4

IBM Spectrum Protect Plus Versão 10.1.4 apresenta novos recursos e atualizações.

Para obter uma lista de novos recursos e atualizações nesta liberação e nas liberações anteriores da Versão 10, consulte [Atualizações do IBM Spectrum Protect Plus](#).

Informações novas e alteradas nessa documentação do produto estão indicadas por uma barra vertical (|) à esquerda da mudança.

Envolvendo-se no desenvolvimento do produto

É possível influenciar o futuro dos produtos do IBM Storage compartilhando os seus insights com as equipes de design e desenvolvimento. Para se envolver, associe-se ao programa do usuário patrocinador ou ao programa beta.

Programa do usuário patrocinador

O programa do usuário patrocinador do IBM Storage permite trabalhar diretamente com designers e desenvolvedores para influenciar a direção dos produtos que você usa.

A IBM convida você a compartilhar a sua experiência e conhecimento. Se associando ao programa, você pode nos ajudar a explorar e potencialmente implementar novos recursos do produto que são importantes para você e para os seus negócios.

Você usa um produto de software do IBM Storage, como o IBM Spectrum Protect Plus?

Você está pronto para compartilhar a sua visão?

Em seguida, inscreva-se no programa do usuário patrocinador para participar do processo de inovação do produto. Além disso, como um usuário patrocinador, é possível visualizar as liberações de armazenamento futuras e participar de programas beta para testar novos recursos do produto.

Para se associar ao programa do usuário patrocinador ou para obter informações adicionais, complete o formulário a seguir:

[IBM Usuário do Patrocinador de Armazenamento](#)

As suas informações permanecerão confidenciais e serão usadas pelas equipes de design e desenvolvimento da IBM somente para propósitos de desenvolvimento do produto.

Programa beta

O programa beta IBM Spectrum Protect Plus fornece uma primeira visão dos futuros recursos do produto e uma chance de influenciar mudanças de design. É possível testar o novo software em seu ambiente e participar ativamente do processo de desenvolvimento do produto.

O programa beta atrai uma ampla gama de participantes, incluindo clientes, Parceiros de Negócios IBM e funcionários do IBM.

O programa oferece os seguintes benefícios:

Obter acesso ao código inicial e avaliar novos recursos e aprimoramentos do produto

Você tem acesso ao código beta antes da disponibilidade geral da liberação do produto, para determinar se os novos recursos e aprimoramentos são um bom ajuste para sua organização. Depois que o código for transferido por download, é possível executar e validar o novo software em seu ambiente. Será possível, então, identificar e resolver quaisquer problemas antes que o código esteja disponível, economizando tempo e ajudando a evitar problemas de produção posteriores. Quando o código ficar disponível, você estará pronto para realizar a instalação e aproveitar as vantagens dos novos recursos.

Interaja com as equipes de design e de desenvolvimento

Os designers, arquitetos, desenvolvedores e testadores de produto ajudam a planejar a liberação beta e suportar seus participantes. Esses especialistas podem ajudá-lo a resolver quaisquer problemas.

Torne-se um cliente de referência do IBM

Após sua experiência positiva com o código beta, o IBM convidará você para participar do programa de referência. A equipe de marketing do IBM ajuda a criar uma mensagem para permitir que outros testadores beta potenciais saibam sobre seu sucesso em adotar e usar o código inicial.

Informações de contato e inscrição

Para obter mais informações sobre o programa beta, entre em contato com Mary Anne Filosa em <mailto:mfilosa@us.ibm.com>.

É possível se inscrever, preenchendo o [Formulário de inscrição do programa beta do IBM Spectrum Protect Plus](#).

Capítulo 1. Visão geral do IBM Spectrum Protect Plus

O IBM Spectrum Protect Plus é uma solução de proteção e disponibilidade de dados para ambientes virtuais e aplicativos de banco de dados que podem ser implementados em minutos e proteger seu ambiente em uma hora.

O IBM Spectrum Protect Plus pode ser implementado como uma solução independente ou integrado com o armazenamento em nuvem ou um servidor do repositório, como um Servidor IBM Spectrum Protect para transferir cópias para armazenamento de longo prazo.

Componentes do Produto

A solução do IBM Spectrum Protect Plus é fornecida como um dispositivo virtual autocontido que inclui componentes de armazenamento e de movimentação de dados.

Requisitos de dimensionamento de componentes: Alguns ambientes podem requerer mais instâncias desses componentes para suportar cargas de trabalho maiores. Para obter orientação sobre como dimensionar, construir e integrar componentes no ambiente IBM Spectrum Protect Plus, consulte o [Blueprints do IBM Spectrum Protect Plus](#).

A seguir estão os componentes de base do IBM Spectrum Protect Plus:

IBM Spectrum Protect Plus Server

Este componente gerencia o sistema inteiro. O servidor consiste em vários catálogos que rastreiam vários aspectos do sistema, como pontos de restauração, configuração, permissões e customizações. Geralmente, há um dispositivo IBM Spectrum Protect Plus em uma implementação, mesmo que a implementação seja distribuída entre vários locais.

O servidor IBM Spectrum Protect Plus contém um servidor vSnap integrado e um servidor proxy VMware vStorage API for Data Protection (VADP). Para ambientes de backup menores, esses servidores podem ser suficientes. No entanto, para ambientes maiores, mais servidores podem ser necessários.

O servidor vSnap integrado pode ser usado para fazer backup e restaurar um pequeno número de máquinas virtuais e avaliar operações do IBM Spectrum Protect Plus. À medida que seus requisitos para backup e restauração de dados crescem, o armazenamento do vSnap pode ser expandido incluindo servidores vSnap externos. Ao incluir servidores vSnap externos em seu ambiente, é possível reduzir a carga no dispositivo IBM Spectrum Protect Plus.

Site

Este componente é uma construção de política do IBM Spectrum Protect Plus que é usada para gerenciar a colocação de dados no ambiente. Um site pode ser físico, como um data center, ou lógico, como um departamento ou organização. Os componentes do IBM Spectrum Protect Plus são designados a sites para localizar e otimizar caminhos de dados. Uma implementação sempre possui pelo menos um site por local físico. O método preferencial é localizar a movimentação de dados para sites, colocando servidores vSnap e proxies VADP juntos em um único site. A colocação de dados de backup em um site é controlada por políticas de acordo de nível de serviço (ANS).

servidor vSnap

Este componente é um conjunto de armazenamento em disco que recebe dados de sistemas de produção com o propósito de proteção ou reutilização de dados. O servidor vSnap consiste em um ou mais discos e pode ser submetido a scale-up (incluir discos para aumentar a capacidade) ou scale-out (introduzir vários servidores vSnap para aumentar o desempenho geral). Cada site pode incluir um ou mais servidores vSnap.

Conjunto do vSnap

Este componente é a organização lógica de discos em um conjunto de espaço de armazenamento, que é usado pelo componente do servidor vSnap. Esse componente também é referido como um conjunto de armazenamentos.

proxy VADP

Esse componente é responsável por mover dados dos armazenamentos de dados do vSphere para fornecer proteção para máquinas virtuais VMware e é requerido apenas para proteção de recursos do VMware. Cada site pode incluir um ou mais proxies VADP.

Interfaces com o usuário

O IBM Spectrum Protect Plus fornece as seguintes interfaces para tarefas de configuração, administrativas e de monitoramento:

IBM Spectrum Protect Plus interface com o usuário

A interface com o usuário do IBM Spectrum Protect Plus é a interface primária para configurar, administrar e monitorar operações de proteção de dados.

Um componente principal da interface é o painel, que fornece informações de resumo sobre o funcionamento de seu ambiente. Para obter mais informações sobre o painel, consulte [“Painel do Produto” na página 3](#).

A barra de menus na interface com o usuário contém os seguintes itens:

 Ícone Alertas	Este ícone abre a janela Alertas . Para obter mais informações sobre alertas, consulte “Alertas” na página 4 .
 Ícone de ajuda	Este ícone abre o sistema de ajuda on-line.
Menu do usuário	Este menu mostra o nome do usuário que está com logon efetuado. O menu fornece acesso a informações e à documentação do produto, a logs e à opção de saída do usuário.

interface da linha de comandos vSnap

A interface da linha de comandos do vSnap é uma interface secundária para administrar algumas tarefas de proteção de dados. Execute o comando **vsnap** para acessar a interface da linha de comandos. O comando pode ser chamado pelo ID do usuário `serveradmin` ou por qualquer outro usuário do sistema operacional que tenha privilégios de administrador do vSnap.

Console Administrativo

O console administrativo é usado para instalar correções e atualizações de software e para concluir outras tarefas administrativas, como gerenciar certificados de segurança, iniciar e parar o IBM Spectrum Protect Plus e mudar o fuso horário para o aplicativo.

Exemplo de implementação

A figura a seguir mostra IBM Spectrum Protect Plus implementado em dois locais ativos. Cada local tem um inventário que requer proteção. O Local 1 tem um servidor vCenter e dois data centers do vSphere (e um inventário de máquinas virtuais) e o Local 2 tem um único data center (e um inventário menor de máquinas virtuais).

O servidor IBM Spectrum Protect Plus é implementado em apenas um dos sites. Os proxies VADP e servidores vSnap (com seus discos correspondentes) são implementados em cada site para localizar a movimentação de dados no contexto dos recursos protegidos do vSphere.

A replicação bidirecional está configurada para ficar entre os servidores vSnap nos dois sites.

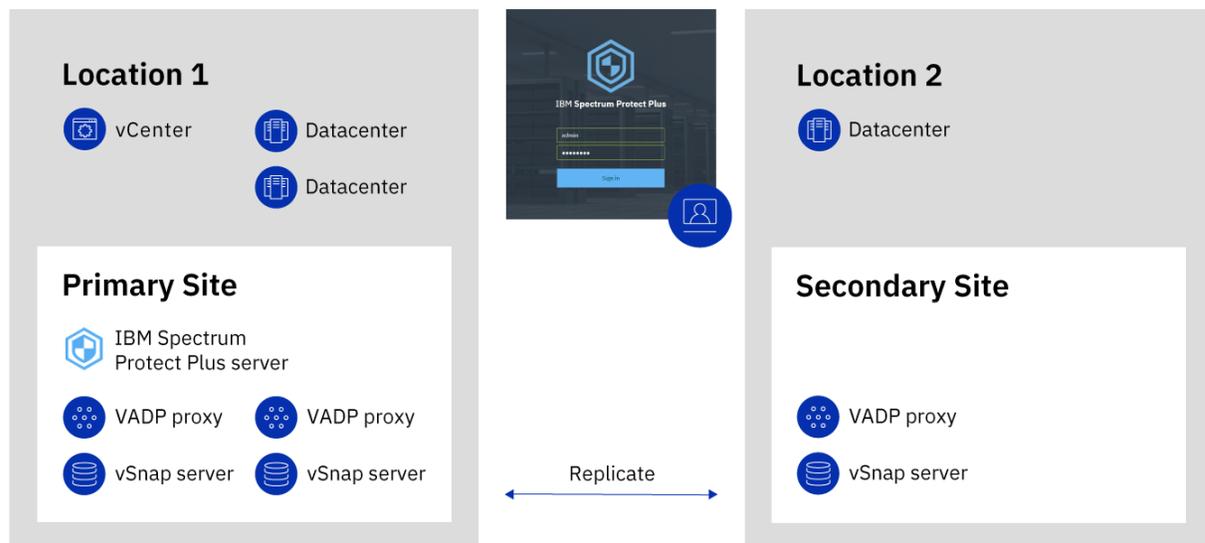


Figura 1. IBM Spectrum Protect Plus implementação em duas localizações geográficas

Painel do Produto

O painel do IBM Spectrum Protect Plus resume o funcionamento de seu ambiente virtual em três seções: **Tarefas e operações**, **Destinos** e **Cobertura**.

Tarefas e Operações

A seção **Tarefas e operações** mostra um resumo de atividades da tarefa para um período de tempo selecionado. Selecione o período de tempo da lista suspensa. As seguintes informações são mostradas nesta seção:

Atualmente em execução

A seção **Atualmente em execução** mostra o número total de tarefas que estão em execução e a porcentagem de uso da unidade do processador central (CPU) no dispositivo virtual IBM Spectrum Protect Plus. Essa porcentagem é atualizada a cada 10 segundos.

Para visualizar informações detalhadas sobre tarefas em execução, clique em **Visualizar**.

Histórico

A seção **Histórico** mostra o número total de tarefas que foram concluídas dentro do período de tempo selecionado. Este número não inclui tarefas em execução.

Esta seção também mostra a taxa de sucesso para tarefas durante o período de tempo selecionado. A taxa de sucesso é calculada usando a seguinte fórmula:

$$100 \times \text{Tarefas bem-sucedidas} / \text{Total de tarefas} = \text{Taxa de sucesso}$$

As tarefas concluídas são mostradas por status da tarefa:

Bem-sucedida

O número de tarefas que foram concluídas sem avisos ou erros críticos.

Com Falha

O número de tarefas que falharam com erros críticos ou que falharam ao serem concluídas.

Advertência

O número de tarefas que foram concluídas parcialmente, ignoradas ou, de outra forma, resultaram em avisos.

Para visualizar informações detalhadas do histórico da tarefa, clique em **Visualizar**.

Destinos

A seção **Destino** mostra um resumo dos dispositivos que são usados para operações de backup. As seguintes informações são mostradas nesta seção:

Resumo de Capacidade

A seção **Resumo de capacidade** mostra o uso e a disponibilidade atuais dos servidores vSnap que estão disponíveis para o IBM Spectrum Protect Plus.

Para visualizar informações sobre servidores vSnap, clique em **Visualizar**.

Status de Dispositivo

A seção **Status do dispositivo** mostra o número total de dispositivos que estão disponíveis para uso.

O número de dispositivos que estão off-line ou, de outra forma, indisponíveis é mostrado no campo **Inativo**.

O número de dispositivos que estão na capacidade é mostrado no campo **Cheio**.

Redução de Dados

A seção **Redução de dados** mostra proporções de deduplicação de dados e de compactação de dados.

A proporção de deduplicação de dados é a quantidade de dados que são protegidos em comparação com o espaço físico que é necessário para armazenar os dados após a remoção de duplicatas. Essa proporção representa economia de espaço adicional obtida sobre a proporção de compactação. Se a deduplicação estiver desativada, essa proporção será 1.

Cobertura

A seção **Cobertura** mostra um resumo dos recursos que são inventariados pelo IBM Spectrum Protect Plus e as políticas de acordo de nível de serviço (ANS) que são designadas aos recursos. As seguintes informações são mostradas nesta seção:

Proteção de Origem

A seção **Proteção de origem** mostra o número total de recursos de origem, como máquinas virtuais e servidores de aplicativos, que são inventariados no catálogo do IBM Spectrum Protect Plus. É mostrado o número de recursos protegidos e desprotegidos.

Esta seção também mostra a proporção de recursos que são protegidos no IBM Spectrum Protect Plus para o total de recursos, expresso como um percentual.

Policies

A seção **Políticas** mostra o número total de políticas de ANS com tarefas de proteção associadas.

Esta seção também mostra as três políticas de ANS que têm os recursos designados de contagem mais alta.

Para visualizar informações detalhadas sobre todas as políticas de ANS, clique em **Visualizar**.

Alertas

O menu **Alertas** exibe avisos e erros atuais e recentes no ambiente IBM Spectrum Protect Plus. O número de alertas é exibido em um círculo vermelho, indicando que os alertas estão disponíveis para visualização.

Clique no menu **Alertas** para visualizar a lista de alertas. Cada item na lista inclui um ícone de status, um resumo do alerta, a hora em que ocorreu o aviso ou o erro associado e um link para visualizar os logs associados.

A lista de alertas pode incluir os seguintes tipos de alerta:

Tipos de Alerta

Tarefa com falha

É exibido quando uma tarefa falha.

Tarefa parcialmente bem-sucedida

É exibido quando uma tarefa é bem-sucedida parcialmente.

Espaço baixo do disco do sistema

É exibido quando a quantidade de espaço livre em disco é 10% ou menos.

espaço de armazenamento vSnap baixo

É exibido quando a quantidade de espaço livre em disco é 10% ou menos.

Memória baixa do sistema

É exibido quando o uso de memória excede 95%.

Alto uso de CPU do sistema

É exibido quando o uso do processador excede 95%.

VM do hypervisor não localizada

É exibido quando a VM não é localizada.

Exceção de captura instantânea de armazenamento de replicação bloqueada

É exibido quando a captura instantânea de armazenamento de replicação está bloqueada. Aumente a retenção de replicação ou aumente a política de frequência de replicação.

Exceção de captura instantânea de armazenamento de transferência bloqueada

É exibido quando a captura instantânea de armazenamento transferida mais recentemente está bloqueada. Aumente a retenção de transferência ou aumente a política de frequência de transferência.

Falha de backup do log SQL

É exibido quando o backup do log falha para um banco de dados.

Falha de backup de SMO do log SQL

É exibido quando há uma falha de backup do log de transações do Server Management Object.

Tamanho do log SQL muito grande

É exibido quando o tamanho do log de transações é maior que o espaço disponível no disco.

Espaço restante baixo do log SQL

É exibido quando o diretório temporário de backup do log de transações é baixo no espaço em disco e exibe a quantidade de espaço restante.

Controle de Acesso Baseado na Função

O controle de acesso baseado em função define os recursos e permissões que estão disponíveis para contas do usuário do IBM Spectrum Protect Plus.

O acesso baseado em função fornece aos usuários acesso apenas às características e recursos que eles requerem. Por exemplo, uma função pode permitir que um usuário execute tarefas de backup e restauração para recursos do hypervisor, mas não permite que o usuário conclua tarefas administrativas, como criar ou modificar contas do usuário.

Para concluir as tarefas que estão descritas nesta documentação, o usuário deve pertencer a uma função que tenha as permissões necessárias. Certifique-se de que sua conta do usuário pertença a uma função que tem as permissões necessárias antes de iniciar a tarefa.

Para configurar e gerenciar o acesso de usuário, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#).

Replicar dados de armazenamento de backup

Ao ativar a replicação de dados de backup, os dados de um servidor vSnap são replicados de forma assíncrona para outro servidor vSnap. Por exemplo, é possível replicar dados de backup de um servidor vSnap em um site primário para um servidor vSnap em um site secundário.

Ativando a replicação de dados de armazenamento de backup

Ative a replicação de dados de armazenamento de backup executando as seguintes ações:

1. Estabeleça uma parceria de replicação entre servidores vSnap. As parcerias de replicação são estabelecidas na área de janela Gerenciar de um servidor vSnap registrado. Na seção **Configurar parceiros de armazenamento**, selecione outro servidor vSnap registrado como um parceiro de armazenamento para servir como o destino das operações de replicação.

Certifique-se de que o conjunto no servidor parceiro seja grande o suficiente para conter dados replicados do conjunto do servidor principal.

2. Ative a replicação de dados de armazenamento de backup. O recurso de replicação é ativado usando políticas de backup, que também são referidas como políticas de acordo de nível de serviço (ANS). Essas políticas definem parâmetros que são aplicados a tarefas de backup, incluindo a frequência de operações de backup e a política de retenção para os backups. Para obter informações adicionais sobre políticas de ANS, consulte [Capítulo 6, “Gerenciar políticas SLA para operações de backup”](#), na página 89.

É possível definir as opções de replicação de armazenamento de backup na seção **Proteção operacional > Política de replicação** de uma política de ANS. As opções incluem a frequência da replicação, o site de destino e a retenção da replicação.

Considerações para ativar a replicação de dados de armazenamento de backup

Revise as considerações para ativar a replicação de dados de armazenamento de backup:

- Se seu ambiente incluir uma mistura de servidores vSnap criptografados e não criptografados, selecione **Usar somente armazenamento em disco criptografado** para replicar dados para servidores vSnap criptografados. Se esta opção estiver selecionada e nenhum servidor vSnap criptografado estiver disponível, a tarefa associada falhará.
- Para criar cenários de replicação de um para muitos, em que um único conjunto de dados de backup é replicado para vários servidores vSnap, crie várias políticas de ANS para cada site de replicação.

Transfload para armazenamento de backup secundário

O servidor vSnap é o local de backup primário para capturas instantâneas. Todos os ambientes do IBM Spectrum Protect Plus têm pelo menos um servidor vSnap. Opcionalmente, é possível transferir capturas instantâneas de um servidor vSnap para o armazenamento de backup secundário.

Os destinos de armazenamento de backup secundário a seguir estão disponíveis para operações de transferência:

- IBM Cloud Object Storage (incluindo IBM Cloud Object Storage Systems)
- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure
- Servidores de repositório (para a liberação atual do IBM Spectrum Protect Plus, o servidor do repositório deve ser um Servidor IBM Spectrum Protect)

Esses destinos suportam os tipos de armazenamento a seguir. O tipo de armazenamento que você usa depende de fatores como o tempo de recuperação e os objetivos de segurança.

Armazenamento de objeto

O armazenamento de objeto é um método de armazenamento de dados em que os dados são armazenados como unidades discretas, ou objetos, em um conjunto de armazenamentos ou repositório que não usa uma hierarquia de arquivos, mas que armazena todos os objetos no mesmo nível.

O armazenamento de objeto é uma opção ao transferir dados para um Servidor IBM Spectrum Protect ou um sistema de armazenamento em nuvem. Quando os dados de captura instantânea são transferidos para o armazenamento de objeto, uma cópia completa é criada durante a primeira operação de transferência. As cópias subsequentes são incrementais e capturam mudanças acumulativas desde a última transferência.

A transferência de capturas instantâneas para o armazenamento de objeto é útil se você deseja tempos de backup e recuperação relativamente rápidos e não requer os benefícios de proteção, custo e segurança de prazo mais longo que são fornecidos por armazenamento de archive em fita ou em nuvem.

Armazenamento de archive em fita ou nuvem

O armazenamento em fita significa que os dados são armazenados na mídia de fita física ou em uma biblioteca de fitas virtual. O armazenamento em fita é uma opção quando você transfere dados para um Servidor IBM Spectrum Protect . Armazenando volumes de fita em um local externo seguro que não está conectado à Internet, é possível ajudar a proteger seus dados contra ameaças on-line, como malware e hackers.

O armazenamento de archive em nuvem é um método de armazenamento de longo prazo que copia dados para um dos serviços de armazenamento a seguir: Amazon Glacier, IBM Cloud Object Storage Archive Tier ou Microsoft Azure Archive.

Quando você transfere dados para uma fita ou para um sistema de armazenamento em nuvem, uma cópia completa dos dados é criada.

A transferência de capturas instantâneas para armazenamento de archive em fita ou em nuvem fornece benefícios extras de custo e segurança. No entanto, como a transferência para esses tipos de armazenamento requer uma cópia completa de dados, o tempo necessário para copiar os dados aumenta. Além disso, o tempo de recuperação pode ser imprevisível e os dados podem levar mais tempo para serem processados antes de serem utilizáveis.

Para obter informações sobre como os dados de captura instantânea são copiados para armazenamento de objeto e armazenamento de arquivamento para cada sistema de armazenamento em nuvem, consulte [“Requisitos de nuvem” na página 20](#).

Incluindo armazenamento de backup secundário e criando políticas de backup

Para transferir dados para o armazenamento secundário, as seguintes ações são necessárias:

Ação	Como
<p>Para transferir dados para um servidor de repositório</p> <ul style="list-style-type: none"> • Configure o IBM Spectrum Protect Plus como um cliente de objeto no ambiente Servidor IBM Spectrum Protect . • Inclua o armazenamento em IBM Spectrum Protect Plus. 	<p>Consulte “Configurando um Servidor IBM Spectrum Protect como um destino de transferência” na página 262 e “Incluindo um servidor do repositório como um provedor de armazenamento de backup” na página 267.</p>
<p>Para transferir dados para um armazenamento em nuvem, inclua o armazenamento no IBM Spectrum Protect Plus.</p>	<p>Siga as instruções para seu tipo de armazenamento selecionado:</p> <ul style="list-style-type: none"> • “Incluindo um armazenamento em nuvem do Amazon S3 como um provedor de armazenamento de backup” na página 257 • “Incluindo o IBM Cloud Object Storage como um provedor de armazenamento de backup” na página 259 • “Incluindo armazenamento em nuvem do Microsoft Azure como um provedor de armazenamento de backup” na página 260 • “Incluindo um servidor do repositório como um provedor de armazenamento de backup” na página 267

Ação	Como
Crie uma política de backup que inclua o armazenamento.	Consulte “Criar políticas de backup” na página 73.

Exemplos de Implementações

A figura a seguir mostra IBM Spectrum Protect Plus implementado em dois locais ativos. Cada local tem um inventário que requer proteção. O Local 1 tem um servidor vCenter e dois data centers do vSphere (e um inventário de máquinas virtuais) e o Local 2 tem um único data center (e um inventário menor de máquinas virtuais).

O servidor IBM Spectrum Protect Plus é implementado em apenas um dos sites. Os proxies VADP e servidores vSnap (com seus discos correspondentes) são implementados em cada site para localizar a movimentação de dados no contexto dos recursos protegidos do vSphere.

A replicação bidirecional é configurada para ocorrer entre os servidores vSnap nos dois sites.

As capturas instantâneas são transferidas do servidor vSnap no site secundário para o armazenamento em nuvem para proteção de dados de longo prazo.

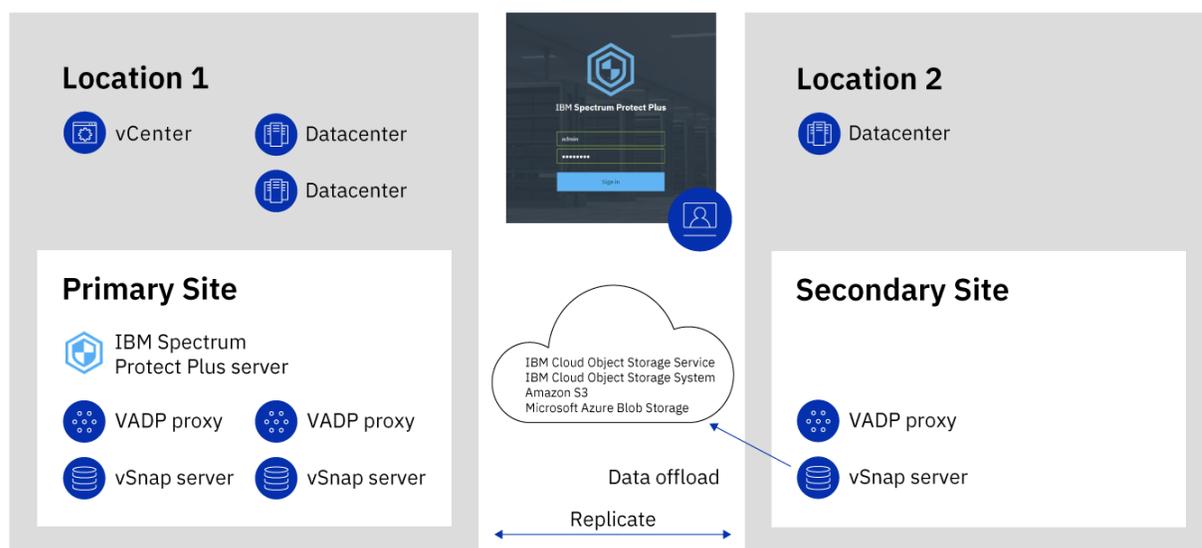


Figura 2. Implementação do IBM Spectrum Protect Plus em duas localizações geográficas com transferência para o armazenamento em nuvem

A figura a seguir mostra a mesma implementação que a figura anterior.

No entanto, nesta implementação, as capturas instantâneas são transferidas do servidor vSnap no site secundário para o IBM Spectrum Protect para proteção de dados de longo prazo.

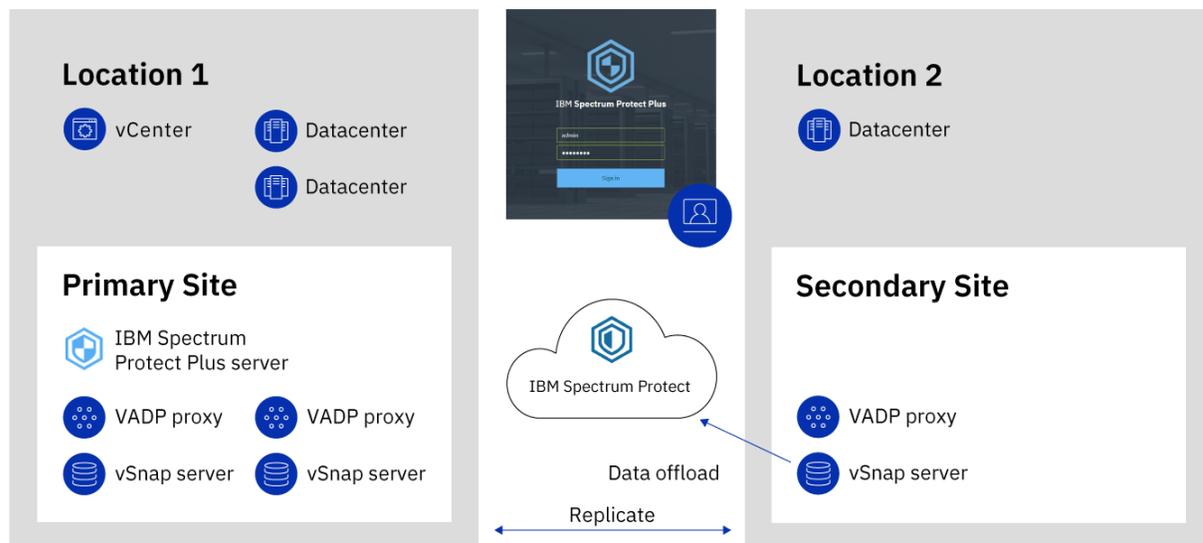


Figura 3. Implementação do IBM Spectrum Protect Plus em duas localizações geográficas com transferência para o IBM Spectrum Protect

IBM Spectrum Protect Plus no IBM Cloud

IBM Spectrum Protect Plus está disponível como um serviço IBM Cloud para VMware Solutions , IBM Spectrum Protect Plus no IBM Cloud.

O IBM Cloud para VMware Solutions permite integrar ou migrar cargas de trabalho do VMware no local para o IBM Cloud usando a infraestrutura escalável do IBM Cloud e a tecnologia de virtualização híbrida do VMware.

IBM Cloud para VMware Solutions fornece os seguintes benefícios principais:

alcance global

Expanda sua área de cobertura de nuvem híbrida para um máximo de 30 data centers de classe corporativa do IBM Cloud no mundo.

Integração aperfeiçoada

Use o processo aperfeiçoado para integrar a nuvem híbrida com a infraestrutura do IBM Cloud.

Implementação e configuração automatizadas

Implemente um ambiente VMware de classe corporativa com Servidores Bare Metal on-demand do IBM Cloud e servidores virtuais usando a implementação e configuração automatizadas do ambiente VMware.

Simplificação

Use uma plataforma de nuvem VMware sem identificar, obter, implementar e gerenciar a computação física subjacente, o armazenamento e a infraestrutura de rede e as licenças de software.

Flexibilidade de expansão e contração

Expanda e comprima as cargas de trabalho do VMware, de acordo com suas necessidades de negócios.

Console de gerenciamento único

Use um único console para implementar, acessar e gerenciar os ambientes VMware no IBM Cloud.

Recursos disponíveis em IBM Spectrum Protect Plus no IBM Cloud

O IBM Spectrum Protect Plus suporta ambientes VMware e Microsoft Hyper-V.

No entanto, o IBM Spectrum Protect Plus no IBM Cloud suporta apenas ambientes VMware.

Esta documentação inclui tópicos sobre recursos que são específicos do Hyper-V. Esses recursos não estarão disponíveis se você estiver usando o IBM Spectrum Protect Plus no IBM Cloud.

A versão atual do IBM Spectrum Protect Plus e do IBM Spectrum Protect Plus no IBM Cloud pode não ser a mesma. Para localizar a documentação para a versão do IBM Spectrum Protect Plus no IBM Cloud que está sendo usada, acesse o [documentação on-line do produto](#) e selecione a versão do produto.

Para obter mais informações

Para obter informações sobre como solicitar, instalar e configurar o IBM Spectrum Protect Plus no IBM Cloud, consulte a documentação a seguir. Um IBMid é necessário para acessar a documentação.

- [Introdução ao IBM Cloud for VMware Solutions](#)
- [Componentes e considerações para o IBM Spectrum Protect Plus no IBM Cloud](#)
- [Gerenciando o IBM Spectrum Protect Plus no IBM Cloud](#)

IBM Spectrum Protect Plus na plataforma de nuvem AWS

O IBM Spectrum Protect Plus na plataforma de nuvem Amazon Web Services (AWS) é uma solução para os usuários que executam o IBM Spectrum Protect Plus no local, mas desejam proteger os bancos de dados que estão em execução na nuvem do AWS.

IBM Spectrum Protect Plus no AWS é uma solução híbrida na qual o servidor IBM Spectrum Protect Plus está no local e o servidor vSnap está no AWS.

A política, a administração do sistema, o controle de acesso e outros recursos do IBM Spectrum Protect Plus são gerenciados e mantidos pelo servidor IBM Spectrum Protect Plus no local. Os dados dos bancos de dados que estão no AWS são, então, armazenados no servidor vSnap que também está no AWS.

Implementando o IBM Spectrum Protect Plus no AWS

O [Página do IBM Spectrum Protect Plus no AWS Marketplace](#) fornece os modelos do AWS CloudFormation que são necessários para implementar o servidor vSnap no AWS, além de informações sobre precificação, uso e suporte. Siga as instruções nessa página e no [Guia de Implementação do IBM Spectrum Protect Plus na Nuvem do AWS](#) para configurar os ambientes local e do AWS.

A implementação do IBM Spectrum Protect Plus no AWS inclui o IBM Spectrum Protect Plus versão 10.1.3. Se desejar usar a versão atual do IBM Spectrum Protect Plus, siga as instruções em [Capítulo 5, “Atualizando componentes do IBM Spectrum Protect Plus”](#), na página 83 para concluir um upgrade.

Capítulo 2. Instalando o IBM Spectrum Protect Plus

Antes de instalar o IBM Spectrum Protect Plus, revise os requisitos do sistema e os procedimentos de instalação.

Roteiro de implementação do produto

Siga o roteiro para instalar, configurar e começar a usar o IBM Spectrum Protect Plus.

Ação	Como
Certifique-se de que seu ambiente do sistema atenda aos requisitos de hardware e de software.	Consulte “Requisitos de Sistema” na página 11.
Determine como dimensionar, construir e posicionar os componentes no ambiente IBM Spectrum Protect Plus.	Consulte o Blueprints do IBM Spectrum Protect Plus .
Instale o IBM Spectrum Protect Plus.	Consulte Capítulo 2, “Instalando o IBM Spectrum Protect Plus” , na página 11.
Se forem necessários servidores vSnap adicionais para suportar seu ambiente, instale e configure os servidores.	Consulte Capítulo 3, “Instalando e configurando servidores vSnap” , na página 53.
Se forem necessários proxies VMware vStorage API for Data Protection (VADP) adicionais para suportar seu ambiente, crie e configure os proxies.	Consulte “Gerenciando proxies de backup do VADP” na página 107.
Conclua as etapas básicas para configurar e começar a usar o IBM Spectrum Protect Plus.	Consulte Capítulo 4, “Desiniciando para um Início Rápido” , na página 69.

Requisitos de Sistema

Antes de instalar o IBM Spectrum Protect Plus, revise os requisitos de hardware e de software para o produto e outros componentes que você planeja instalar no ambiente de armazenamento.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

Para determinar como dimensionar, construir e posicionar os componentes que estão listados nas especificações em seu ambiente IBM Spectrum Protect Plus, consulte o [Blueprints do IBM Spectrum Protect Plus](#).

Requisitos do Componente

Certifique-se de que tenha a configuração do sistema necessária e um navegador suportado para implementar e executar o IBM Spectrum Protect Plus.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

O suporte do IBM Spectrum Protect Plus para plataformas de terceiros, aplicativos, serviços e hardware compara-se com o dos fornecedores de terceiros. Quando um produto ou versão de fornecedor de

terceiros entra no suporte estendido, no suporte de autoatendimento ou no término de vida útil, o IBM Spectrum Protect Plus suporta-o no mesmo nível.

Instalação da máquina virtual

IBM Spectrum Protect Plus é instalado como um dispositivo virtual. Antes de implementar o IBM Spectrum Protect Plus no host, assegure-se de que os requisitos a seguir tenham sido atendidos:

- vSphere 5.5, 6.0, 6.5 ou 6.7
- Microsoft Hyper-V Server 2016 ou Hyper-V 2019.

Para implementação inicial, configure seu dispositivo virtual para atender aos requisitos mínimos a seguir:

- Máquina 8-core de 64 bits
- 48 GB de memória
- 536 GB de armazenamento em disco para a máquina virtual

Use um servidor Network Time Protocol (NTP) para sincronizar os fusos horários entre os recursos do IBM Spectrum Protect Plus que estão em seu ambiente, como o dispositivo virtual do IBM Spectrum Protect Plus, as matrizes de armazenamento, os hypervisores e os servidores de aplicativos. Se os clocks nos vários sistemas estiverem significativamente fora de sincronização, podem ocorrer erros durante tarefas de registro do aplicativo, de catalogação de metadados, de inventário, de backup, de restauração ou de restauração de arquivos. Para obter informações adicionais sobre como identificar e resolver desvios do cronômetro, consulte o seguinte artigo da base de conhecimento do VMware: [Tempo em desvios de máquina virtual devido a desvios do cronômetro de hardware.](#)

Suporte ao navegador

Execute o IBM Spectrum Protect Plus a partir de um computador que tenha acesso ao dispositivo virtual instalado. O IBM Spectrum Protect Plus foi testado com relação aos seguintes navegadores da web. Observe que as versões mais recentes do navegador também podem ser suportadas.

- Firefox 55.0.3
- Google Chrome 60.0.3112 e mais recente
- Microsoft Edge 40.15063/Microsoft EdgeHTML 15.15063 e mais recente

Se a sua resolução de tela for menor que 1024 x 768 pixels, alguns itens podem não caber na janela. As janelas pop-up devem ser ativadas em seu navegador para acessar o sistema de ajuda e algumas operações do IBM Spectrum Protect Plus.

Requisitos do IBM Spectrum Protect

Se você planeja usar o IBM Spectrum Protect como um servidor do repositório para operações de transferência em nuvem, assegure-se de que esteja usando o IBM Spectrum Protect V8.1.8.

Portas do IBM Spectrum Protect Plus

As seguintes portas são usadas pelo IBM Spectrum Protect Plus e por serviços associados. As portas que são indicadas por "Aceitar" na coluna Regra de firewall usam conexões seguras (HTTPS ou SSL).

Tabela 1. Conexões de firewall de entrada (dispositivo IBM Spectrum Protect Plus)

Porta	Protocolo	Firewall	Serviço	Descrição
22	TCP	Aceitar	OpenSSH 5.3 (protocolo 2.0)	Usado para resolução de problemas do IBM Spectrum Protect Plus
443	TCP	Aceitar	Um microsserviço executando um proxy reverso	Ponto de entrada principal para as conexões do cliente (SSL)
5671	TCP, AMQP	Aceitar	RabbitMQ	Estrutura de mensagem usada para gerenciar mensagens produzidas e consumidas pelo proxy VADP e por trabalhadores de gerenciamento de tarefas do VMware. Além disso, facilita o gerenciamento de log da tarefa.
8090	TCP	Aceitar	Administrative Console Framework (ACF)	Estrutura extensível para funções de administração do sistema. Suporta plug-ins que executam operações, como atualizações do sistema e operações de backup ou restauração do catálogo
8761	TCP	Aceitar	Servidor de Descoberta	Descobre automaticamente os proxies VADP e é usado pelas operações de backup de VM do IBM Spectrum Protect Plus

Tabela 2. Conexões de firewall recebidas (servidor vSnap integrado)

Porta	Protocolo	Firewall	Serviço	Descrição
111	TCP	Aceitar	Ligação da Porta RPC	Permite que os clientes descubram portas que os clientes Open Network Computing (ONC) requerem para se comunicar com servidores ONC (internos).
2049	TCP	Aceitar	NFS	Usado para transferência de dados NFS para e do vSnap (interno)
3260	TCP	Aceitar	iSCSI	Usado para transferência de dados iSCSI para e do vSnap (interno)
20048	TCP	Aceitar	NFS	Usado para transferência de dados NFS para e do vSnap (interno)

Tabela 3. Conexões de firewall de saída (dispositivo IBM Spectrum Protect Plus)

Porta	Protocolo	Serviço	Descrição
22	TCP	OpenSSH 5.3 (protocolo 2.0)	Usado para comunicações SSH com servidores remotos que estão executando componentes de aplicativos guest.
25	TCP	SMTP	Serviço de email.
389	TCP	LDAP	Serviços do Active Directory.
443	TCP	Host ESXi do VMware	Porta do host ESXi para gerenciar operações.
443	TCP	vCenter do VMware	Conexões do cliente para vCenter.
636	TCP	LDAP	Serviços de Active Directory (SSL).

Tabela 3. Conexões de firewall de saída (dispositivo IBM Spectrum Protect Plus) (continuação)

Porta	Protocolo	Serviço	Descrição
902	TCP	Serviço VMware NFC	Network File Copy (NFC) fornece um serviço FTP com reconhecimento de tipo de arquivo para componentes do vSphere. Por padrão, o ESXi usa o NFC para operações, como copiar e mover dados entre os armazenamentos de dados.
5985	TCP	Windows Remote Management (WinRM)	Conexões do cliente de aplicativos Hyper-V e guest.
8098	TCP	proxy VADP	Proxy de proteção de dados da máquina virtual.
8900	TCP	vSnap	Versão do OVA/ Instalador da estrutura de armazenamento inteligente usada como um destino para operações de proteção de dados.

Requisitos do servidor vSnap

Um servidor vSnap é o destino de backup primário para o IBM Spectrum Protect Plus. Em um ambiente VMware ou Hyper-V, um servidor vSnap com o nome `localhost` é instalado automaticamente no momento em que o dispositivo virtual do IBM Spectrum Protect Plus é implementado inicialmente. Em ambientes corporativos de backup maiores, podem ser necessários mais servidores vSnap.

Aloque a memória com base na capacidade de backup para deduplicação mais eficiente. Para obter mais informações e orientação de dimensionamento, consulte [IBM Spectrum Protect Plus Blueprints](#).

Para implementação inicial, certifique-se de que sua máquina virtual ou máquina física Linux atenda aos seguintes requisitos mínimos:

- Processador de 8 núcleos de 64 bits
- 32 GB de memória
- 16 GB de espaço livre no sistema de arquivos raiz
- 128 GB de espaço livre em um sistema de arquivos separado montado no seguinte local: `/opt/vsnap-data`

O serviço de Gerenciamento de Rede Linux deve estar instalado e em execução.

Opcionalmente, uma unidade de estado sólido (SSD) melhora o desempenho do backup e da restauração.

- Para melhorar o desempenho de backup, configure o conjunto para usar um ou mais dispositivos de log suportados por uma SSD. Especifique pelo menos dois dispositivos de log para criar um log espelhado para melhorar a redundância.
- Para melhorar o desempenho da restauração, configure o conjunto para usar um dispositivo de cache suportado por uma SSD.

Requisitos de instalação de máquina virtual do servidor vSnap

Antes de implementar o servidor vSnap no host, assegure-se de que os requisitos a seguir estejam no lugar:

- vSphere 5.5, 6.0, 6.5. ou 6.7
- Microsoft Hyper-V 2016 ou Microsoft Hyper-V 2019.

Requisitos de instalação física do servidor vSnap

A partir da V10.1.3, o IBM Spectrum Protect Plus fornece funcionalidade que requer os níveis de kernel suportados no RHEL 7.5 e no CentOS 7.5. Se for necessário usar sistemas operacionais anteriores ao RHEL 7.5 e ao CentOS 7.5, use o IBM Spectrum Protect Plus V10.1.2 para instalações físicas do vSnap V10.1.2.

Os sistemas operacionais Linux a seguir são suportados para instalações físicas do servidor vSnap físico do IBM Spectrum Protect Plus V10.1.4 ou mais recente:

- CentOS 7.1804 (7.5) (x86_64)
- CentOS 7.1810 (7.6) (x86_64)
- RedHat Enterprise Linux 7.5 (x86_64)
- Red Hat Enterprise Linux 7.6 (x86_64)

Se você estiver usando os sistemas operacionais a seguir, use o IBM Spectrum Protect Plus V10.1.2 para instalações físicas do servidor vSnap V10.1.2:

- CentOS Linux7.3.1611 (x86_64)
- CentOS Linux7.4.1708 (x86_64)
- Red Hat Enterprise Linux 7.3 (x86_64)
- Red Hat Enterprise Linux 7.4 (x86_64)

portas do servidor vSnap

As portas a seguir são usadas por servidores vSnap. As portas que são indicadas com Aceitar na coluna Regra de firewall usam conexões seguras (HTTPS/SSL).

Tabela 4. Conexões de firewall vSnap de entrada

Porta	Protocolo	Firewall	Serviço	Descrição
22	TCP	Aceitar	SSH	Usado para resolução de problemas de servidores vSnap
111	TCP	Aceitar	Ligação da Porta RPC	Permite que os clientes descubram portas que os clientes Open Network Connectivity (ONC) requerem para se comunicar com servidores ONC (internos).

Tabela 4. Conexões de firewall vSnap de entrada (continuação)

Porta	Protocolo	Firewall	Serviço	Descrição
137	UDP	Aceitar	SMB/CIFS	Usado para transferência de dados SMB ou CIFS para e de servidores vSnap (internos)
138	UDP	Aceitar	SMB/CIFS	Usado para transferência de dados SMB ou CIFS para e de servidores vSnap (internos)
139	TCP	Aceitar	SMB/CIFS	Usado para transferência de dados SMB ou CIFS para e de servidores vSnap (internos)
445	TCP	Aceitar	SMB/CIFS	Usado para transferência de dados SMB ou CIFS para e de servidores vSnap (internos)
2049	TCP	Aceitar	NFS	Usado para transferência de dados NFS para e de servidores vSnap (internos)
3260	TCP	Aceitar	iSCSI	Usado para transferência de dados iSCSI para e de servidores vSnap (internos)
8900	TCP	Aceitar	HTTPS	APIs de REST do servidor vSnap
20048	TCP	Aceitar	NFS	Usado para transferência de dados NFS para e de servidores vSnap (internos)

Requisitos do proxy do VADP

No IBM Spectrum Protect Plus, a execução de tarefas de backup da máquina virtual por meio do VADP pode consumir recursos do sistema. Criando proxies de tarefa de backup VADP, você ativa o compartilhamento de carga e o balanceamento de carga para as tarefas de backup do IBM Spectrum

Protect Plus. Se os proxies existirem, a carga de processamento inteira será deslocada do dispositivo IBM Spectrum Protect Plus para os proxies.

Esse recurso foi testado somente para ambientes do SUSE Linux Enterprise Server e do Red Hat. O recurso é suportado somente em configurações quad core de 64 bits ou superior com um kernel mínimo de 2.6.32.

Os proxies VADP suportam os seguintes modos de transporte do VMware: Arquivo, SAN, HotAdd, NBDSSL e NBD. Para obter informações adicionais sobre os modos de transporte do VMware, consulte [Métodos de transporte de disco virtual](#).

Esse recurso é suportado somente em configurações quad core de 64 bits ou superior nos ambientes do Linux a seguir:

- Níveis de manutenção e modificação do CentOS Linux 6.5 e mais recentes (iniciando com a correção 1 da versão 10.1.1)
- Níveis de manutenção e modificação do CentOS Linux 7.0 e mais recentes (iniciando com a correção 1 da versão 10.1.1)
- Níveis de manutenção e modificação do Red Hat Enterprise Linux 6, Fix pack 4 e mais recentes
- Níveis de manutenção e modificação do Red Hat Enterprise Linux 7 e mais recentes
- Níveis de manutenção e de modificação do SUSE Linux Enterprise Server 12 e mais recente

Para obter mais informações e orientação de dimensionamento, consulte [Blueprints do IBM Spectrum Protect Plus](#).

Para a implementação inicial de um servidor proxy VADP, assegure-se de que sua máquina Linux atenda aos requisitos mínimos a seguir:

- Processador quad core de 64 bits
- 8 GB de RAM necessário, 16 GB de preferência
- 60 GB de espaço livre em disco

O aumento de CPUs usadas e simultaneidade no servidor proxy VADP requer que a memória que é alocada no servidor proxy seja aumentada de forma apropriada.

O proxy deve ser capaz de montar sistemas de arquivos NFS, que em muitos casos, requer a instalação de um pacote do cliente NFS. Os detalhes exatos do pacote variam com base na distribuição.

Cada proxy deve ter um nome completo do domínio e deve ser capaz de resolver e acessar o vCenter. Os servidores vSnap devem ser acessíveis a partir do proxy. A porta 8098 no servidor proxy VADP deve ser aberta quando o firewall do servidor proxy está ativado.

Portas de proxy do VADP

As seguintes portas são usadas por proxies VADP. As portas que são indicadas com "Aceitar" na coluna Regra de firewall usam conexões seguras (HTTPS ou SSL).

Porta	Protocolo	Firewall	Serviço	Descrição
22	TCP	Aceitar	SSH	A porta 22 é usada para enviar por push o proxy VADP para o nó do host.

Tabela 5. Conexões de firewall do proxy do VADP de entrada (continuação)

Porta	Protocolo	Firewall	Serviço	Descrição
8098	TCP	Aceitar	VADP	Porta padrão para comunicações de API REST baseadas em TLS entre o servidor IBM Spectrum Protect Plus e o proxy VADP.

Tabela 6. Conexões de firewall do proxy do VADP de saída

Porta	Protocolo	Serviço	Descrição
111	TCP	VSnap RPC Port Bind	Permite que clientes descubram portas que clientes ONC requerem para se comunicar com servidores ONC (internas).
443	TCP	Host/vCenter do VMware ESXi	Conexões do cliente para vCenter.
902	TCP	Host ESXi do VMware	A Cópia de Arquivo de Rede (NFC0 fornece um serviço FTP que reconhece o tipo de arquivo para os componentes do vSphere). Por padrão, o ESXi usa NFC para operações, como copiar e mover dados entre armazenamentos de dados.
2049	TCP	vSnap NFS	Usado para compartilhamento de arquivo NFS usando o servidor vSnap.
5671	TCP	RabbitMQ	Estrutura de mensagem usada para gerenciar mensagens que são produzidas e consumidas pelos trabalhadores de gerenciamento de tarefas do proxy VADP e do VMware. Também facilita o log da tarefa.

Tabela 6. Conexões de firewall do proxy do VADP de saída (continuação)

Porta	Protocolo	Serviço	Descrição
8761	TCP	Servidor de Descoberta	Descobre automaticamente proxies VADP e é usado por operações de backup da VM do IBM Spectrum Protect Plus.
20048	TCP	Montagem do vSnap	Monta sistemas de arquivos vSnap em clientes, como o proxy VADP, servidores de aplicativos e armazenamentos de dados de virtualização.

Dica: Os proxies VADP podem ser enviados por push e instalados em servidores baseados no Linux por meio da porta SSH 22.

Se o script de comando de firewall não estiver disponível em seu sistema, edite o firewall manualmente para incluir as portas necessárias e reinicie o firewall. Mais informações sobre a edição de regras de firewall podem ser localizadas aqui, [“Editando portas de firewall”](#) na página 51.

Proxy VADP em requisitos do servidor vSnap

Os proxies VADP podem ser instalados em servidores vSnap no ambiente IBM Spectrum Protect Plus. Uma combinação de proxy VADP e servidor vSnap deve atender aos requisitos mínimos de ambos os dispositivos. Consulte os requisitos do sistema de ambos os dispositivos e inclua os requisitos de núcleo e de RAM juntos para identificar os requisitos mínimos da combinação de proxy VADP e servidor vSnap.

Assegure-se de que a combinação do proxy VADP e do servidor vSnap atenda aos requisitos mínimos recomendados a seguir, que é a soma dos requisitos para cada dispositivo.

Proxy VADP instalado em um servidor vSnap virtual:

- Processador de 8 núcleos de 64 bits
- 48 GB de RAM

Todas as portas necessárias do proxy VADP e do servidor vSnap devem estar abertas na combinação de proxy VADP e servidor vSnap. Revise as seções de portas do proxy VADP e do vSnap dos requisitos do sistema para obter mais informações.

Requisitos de nuvem

Para transferir dados para o armazenamento em nuvem, assegure-se de que seus ambientes do IBM Spectrum Protect Plus e de nuvem atendam aos requisitos a seguir.

Área de cache de disco

Para todas as funcionalidades relacionadas à transferência ou restauração a partir da nuvem, o servidor vSnap requer uma área de cache de disco no servidor vSnap.

- Durante operações de transferência, esse cache é usado como uma área de preparação temporária para objetos que estão com upload pendente para o terminal de nuvem.
- Durante operações de restauração, a área de cache de disco é usada para armazenar em cache os objetos transferidos por download, bem como para armazenar quaisquer dados temporários que possam ser gravados no volume de restauração.

Para obter instruções sobre como dimensionar e instalar o cache, consulte [Configuração de transferência em nuvem](#) ou os [Blueprints do IBM Spectrum Protect Plus](#).

Requisitos de Certificado

- **Certificados autoassinados:** se o terminal de nuvem ou o servidor de repositório usar um certificado autoassinado, o certificado deverá ser especificado (no formato Privacy Enhanced Mail (PEM)) ao registrar a nuvem ou o servidor de repositório na interface com o usuário do IBM Spectrum Protect Plus.
- **Certificados assinados por Autoridade de Certificação privada:** se o terminal de nuvem ou o servidor de repositório usar um certificado assinado por uma Autoridade de Certificação (CA) privada, o certificado de terminal deverá ser especificado (no formato PEM) quando você registrar a nuvem ou o servidor de repositório na interface com o usuário do IBM Spectrum Protect Plus. Além disso, o certificado raiz/intermediário da CA privada deve ser incluído no armazenamento de certificados do sistema em cada servidor vSnap usando o procedimento a seguir:
 1. Efetue login no console do servidor vSnap como o usuário `serveradmin` e faça upload de quaisquer certificados de CA privados (no formato PEM) em um local provisório.
 2. Copie cada arquivo de certificado para o diretório de armazenamento de certificados do sistema (`/etc/pki/ca-trust/source/anchors/`) executando o comando a seguir:

```
$ sudo cp /tmp/private-ca-cert.pem /etc/pki/ca-trust/source/anchors/
```
 3. Para incorporar o certificado customizado recém-incluído e atualizar o pacote configurável de certificados do sistema, execute o comando a seguir:

```
$sudo update-ca-trust
```
- **Certificados assinados pela Autoridade de Certificação pública:** se o terminal de nuvem usar um certificado assinado por CA pública, nenhuma ação especial será necessária. O servidor vSnap valida o certificado usando o armazenamento de certificados do sistema padrão.

Requisitos de Rede

As portas a seguir são usadas para comunicação entre os servidores vSnap e os terminais do servidor em nuvem ou de repositório.

Tabela 7. Conexões de firewall do servidor vSnap de saída

Porta	Protocolo	Serviço	Descrição
443	TCP	HTTPS	Permite que o vSnap se comunique com os terminais do Amazon S3, Azure ou IBM Cloud Object Storage.
9000	TCP	HTTPS	Permite que o vSnap se comunique com os terminais do IBM Spectrum Protect (servidor de repositório).

Quaisquer firewalls ou proxies de rede que executam a Intercepção de SSL Interception ou a Inspeção Abrangente de Pacote para tráfego entre os servidores vSnap e os terminais de nuvem podem interferir na validação de certificado SSL nos servidores vSnap. Essa interferência também pode causar falhas na tarefa de transferência em nuvem. Para evitar essa interferência, os servidores vSnap devem ser isentos da intercepção de SSL e da inspeção na configuração de firewall ou de proxy.

Requisitos do provedor em nuvem

O gerenciamento de ciclo de vida nativo não é suportado. O IBM Spectrum Protect Plus gerencia o ciclo de vida de objetos transferidos por upload automaticamente usando uma abordagem incremental permanente, em que os objetos mais antigos ainda podem ser usados por capturas instantâneas mais recentes. A expiração automática ou manual de objetos fora do IBM Spectrum Protect Plus levará à distorção de dados.

Se o provedor em nuvem usar um certificado SSL que seja autoassinado ou assinado por uma Autoridade de Certificação privada, consulte [Requisitos de certificado](#).

Requisitos de nuvem do Amazon S3

- **Transferência:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, um depósito existente em uma das camadas de armazenamento suportadas deve ser especificado: S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access ou S3 One Zone-Infrequent Access.
- **Archive:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, um depósito existente em uma das camadas de armazenamento suportadas deve ser especificado: S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access ou S3 One Zone-Infrequent Access. O IBM Spectrum Protect Plus fará upload diretamente dos arquivos de dados para a camada do Glacier. Alguns arquivos de metadados pequenos serão armazenados na camada padrão para o depósito. Uma cópia desses arquivos de metadados também é colocada na camada do Glacier para propósitos de recuperação de desastre.

Requisitos do IBM Cloud Object Storage

- **Transferência:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, um depósito existente deve ser especificado. Se o depósito especificado tiver uma política WORM que bloqueia objetos por um determinado período de tempo, o IBM Spectrum Protect Plus detectará automaticamente a configuração e excluirá capturas instantâneas após a política WORM remover o bloqueio.
- **Archive:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, um depósito existente deve ser especificado. Se o depósito especificado tiver uma política WORM que bloqueia objetos por um determinado período de tempo, o IBM Spectrum Protect Plus detectará automaticamente a configuração e excluirá capturas instantâneas após a política WORM remover o bloqueio. O IBM Spectrum Protect Plus cria uma única regra de gerenciamento de ciclo de vida no depósito para migrar arquivos de dados para a camada de archive.

Requisitos do Microsoft Azure

- **Transferência:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, um contêiner existente em uma conta de armazenamento quente ou frio deve ser especificada.
- **Archive:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, um contêiner existente em uma conta de armazenamento quente ou frio deve ser especificado. O IBM Spectrum Protect Plus move os arquivos entre as camadas on demand. Os arquivos de dados serão imediatamente movidos para a camada de archive e retornados temporariamente para a camada quente somente durante uma operação de restauração. Alguns arquivos de metadados pequenos serão armazenados na camada padrão para o contêiner. Uma cópia desses arquivos de metadados também é colocada na camada de archive para propósitos de recuperação de desastre.

Requisitos do IBM Spectrum Protect (servidor de repositório)

- **Transferência:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, não é possível usar um depósito existente. O IBM Spectrum Protect Plus cria um depósito nomeado exclusivamente para seu próprio uso.
- **Archive:** quando o provedor em nuvem é registrado no IBM Spectrum Protect Plus, não é possível usar um depósito existente. O IBM Spectrum Protect Plus cria um depósito nomeado exclusivamente para seu próprio uso. O IBM Spectrum Protect Plus fará upload diretamente dos arquivos de dados para o armazenamento em fita do IBM Spectrum Protect. Alguns arquivos de metadados pequenos serão armazenados no armazenamento de objetos do IBM Spectrum Protect. Uma cópia desses arquivos de metadados também é colocada no armazenamento em fita do IBM Spectrum Protect para propósitos de recuperação de desastre.

Tabela 8. Requisitos de transferência e archive para provedores em nuvem

Operação	Provedor	Requisitos
Transferência	Amazon S3	Um depósito existente deve ser especificado a partir de uma das camadas de armazenamento suportadas.
Transferência	IBM Cloud Storage	Um depósito existente deve ser especificado.
Transferência	Microsoft Azure	Um contêiner existente deve ser especificado a partir da camada de armazenamento quente ou frio.
Transferência	IBM Spectrum Protect	O IBM Spectrum Protect Plus cria seu próprio depósito exclusivo.
Archive	Amazon S3	Permite que o vSnap se comunique com os terminais do IBM Spectrum Protect (servidor de repositório).
Archive	IBM Cloud Storage	Um depósito existente deve ser especificado a partir da camada de archive.
Archive	Microsoft Azure	Um contêiner existente deve ser especificado a partir da camada de armazenamento quente e da camada de archive.
Archive	IBM Spectrum Protect	O IBM Spectrum Protect Plus cria seu próprio depósito exclusivo para ser copiado para o armazenamento em fita do IBM Spectrum Protect.

Para obter informações de iniciação rápida para ajudá-lo a configurar e transferir dados para provedores em nuvem específicos, consulte: [Transferência de dados para armazenamento de objeto de nuvem com IBM Spectrum Protect Plus](#).

Requisitos do Hypervisor

Revise os requisitos do hypervisor para IBM Spectrum Protect Plus.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

requisitos do Hyper-V

O servidor Microsoft Hyper-V deve atender aos seguintes requisitos mínimos:

- Hyper-V Server 2016 ou Microsoft Hyper-V no Windows Server 2016
- Microsoft Hyper-V no Windows Server 2019

O backup e a restauração de discos rígidos virtuais compartilhados (VHDX compartilhado) não são suportados. Para problemas conhecidos e limitações, consulte <https://www.ibm.com/support/docview.wss?uid=ibm10884592>.

O IBM Spectrum Protect Plus não protege os ambientes nos quais o Hyper-V Replica está ativado.

O Serviço Inicializador iSCSI Microsoft deve estar em execução em todos os servidores Hyper-V, incluindo nós do cluster. Na janela **Serviços**, configure o tipo de inicialização para o Microsoft iSCSI Initiator Service como **Automático** para que o serviço esteja disponível quando o servidor Hyper-V ou o nó do cluster for iniciado.

O parâmetro **DiskPart** automount deve ser ativado no servidor Hyper-V. Para obter mais informações sobre como ativar o parâmetro automount, consulte o tópico [Automount](#) no website da Microsoft.

Os servidores Hyper-V podem ser registrados usando um nome de Sistema de Nomes de Domínio (DNS) ou endereço IP. Os nomes de DNS devem ser resolvidos por IBM Spectrum Protect Plus. Se o servidor Hyper-V for parte de um cluster, todos os nós no cluster deverão ser resolvíveis via DNS. Se o DNS não está disponível, deve-se incluir o servidor no arquivo `/etc/hosts` no dispositivo IBM Spectrum Protect Plus usando a linha de comandos. Se mais de um servidor Hyper-V estiver configurado em um ambiente em cluster, será necessário incluir todos os servidores no arquivo `/etc/hosts`. Quando estiver registrando o cluster no IBM Spectrum Protect Plus, registre o Gerenciador de Cluster de Failover.

Requisitos do VMware

As seguintes versões do VMware vSphere são suportadas:

- vSphere 5.5, incluindo todas as atualizações e os níveis de correção
- vSphere 6.0, incluindo todas as atualizações e os níveis de correção
- vSphere 6.5, incluindo todas as atualizações e os níveis de correção
- vSphere 6.7, incluindo todas as atualizações e os níveis de correção

Certifique-se de que a versão mais recente do VMware Tools esteja instalada em seu ambiente. O IBM Spectrum Protect Plus foi testado com o VMware Tools 9.10.0 instalado.

Os volumes Physical RDM (pRDM) não suportam capturas instantâneas. As máquinas virtuais que contêm um ou mais volumes de mapeamento de dispositivo bruto (RDM) que estão equipados no physical-compatibility mode (pRDM) são salvas em backup. No entanto, os volumes pRDM não são processados como parte da operação de backup da máquina virtual.

Requisitos de Indexação de Arquivo e Restauração

Revise os requisitos de indexação e restauração para o IBM Spectrum Protect Plus.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

Os discos iSCSI que são mapeados diretamente para o sistema operacional guest não serão indexados. Os volumes suportados incluem volumes VMDK ou VHD que são montados por meio da configuração da máquina virtual associada.

A quantidade de espaço livre necessária para os metadados no catálogo depende do número total de arquivos presentes no ambiente. Para catalogar um milhão de arquivos, o volume do catálogo no dispositivo IBM Spectrum Protect Plus requer aproximadamente 350 MB de espaço livre por versão retida. O espaço usado pelos metadados de indexação de arquivo é recuperado quando as instâncias de backup correspondentes expiram.

Requisitos do VMware

Nas configurações da máquina virtual em Configuração avançada, a configuração `disk.enableUUID` deve estar presente e ser configurada como `true`.

Requisitos do Windows

Sistemas Operacionais Suportados	<ul style="list-style-type: none">• Windows Server 2008 R2• Windows Server 2012 R2 e Windows Server 2012 R2 core• Windows Server 2016 e Windows Server 2016cCore• Windows Server 2019 e Windows Server 2019 core
Sistemas de Arquivos Suportados	<ul style="list-style-type: none">• NTFS• ReFS• CsvFS
Tipos de armazenamento em disco suportados	Discos básicos com <ul style="list-style-type: none">• Partições MBR• Partições GPT Restrição: O backup ou restauração de arquivos em discos dinâmicos não é suportado.

- O IBM Spectrum Protect Plus suporta apenas os sistemas operacionais disponíveis para seus hypervisors. Revise a documentação do hypervisor para obter informações sobre sistemas operacionais suportados.
- As operações de indexação e de restauração de arquivos suportam discos SCSI em um ambiente Hyper-V. Discos Integrated Drive Electronics (IDE) não são suportados. Observe que as máquinas virtuais de Geração 1 requerem os discos de inicialização IDE; entretanto, se discos SCSI adicionais estiverem disponíveis, as operações de indexação e restauração de arquivo serão suportadas nesses discos.
- O Windows Remote Shell (WinRM) deve estar ativado.

Importante: O IBM Spectrum Protect Plus pode proteger e restaurar máquinas virtuais com outros sistemas de arquivos, mas somente os sistemas de arquivos listados anteriormente são elegíveis para indexação e restauração de arquivo.

- Quando a indexação de arquivo é executada em um ambiente Windows, os diretórios a seguir no recurso são ignorados:

```
\Drivers
\Program Files
\Program Files (x86)
\Windows
\winnt
```

Nota: Os arquivos dentro desses diretórios não são incluídos no inventário do IBM Spectrum Protect Plus e não estão disponíveis para recuperação de arquivo.

- Assegure-se de que a versão mais recente do VMware Tools esteja instalada nas máquinas virtuais VMware e que os Serviços de Integração do Hyper-V estejam instalados em suas máquinas virtuais Hyper-V.

Requisitos de Espaço

- A unidade C:\ deve ter espaço temporário suficiente para salvar os resultados da indexação de arquivo.
- Quando os sistemas de arquivos são indexados, os arquivos de metadados temporários são gerados sob o diretório /tmp e, em seguida, excluídos assim que a indexação é concluída. A quantidade de espaço livre necessário para os metadados depende do número total de arquivos presentes no

sistema. Certifique-se de que haja aproximadamente 350 MB de espaço livre por 1 milhão de arquivos.

Requisitos de Conectividade

- O nome do host do dispositivo IBM Spectrum Protect Plus deve ser resolvível a partir da máquina virtual Windows.
- O endereço IP da máquina virtual selecionada para indexação deve estar visível para o cliente vSphere ou o Hyper-V Manager.
- A máquina virtual Windows selecionada para indexação deve permitir conexões de saída com a porta 22 (SSH) no dispositivo IBM Spectrum Protect Plus.
- Todos os firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor por meio do WinRM.

Requisitos de autenticação e de privilégio

As credenciais que são especificadas para a máquina virtual devem incluir um usuário com os seguintes privilégios:

- A identidade do usuário deve ter o direito de "Efetuar logon como um serviço", que é designado por meio do painel de controle de Ferramentas administrativas na máquina local (**Política de segurança local > Políticas locais > Designação de direitos do usuário > Efetuar logon como um serviço**).

Para obter mais informações sobre o direito "Efetuar logon como um serviço", consulte [Incluir o direito Efetuar logon como um serviço em uma conta](#).

- A política de segurança padrão usará o protocolo NTLM do Windows e a identidade do usuário seguirá o formato padrão `domain\Name` se a máquina virtual Hyper-V estiver conectada a um domínio. O formato `<local administrator>` será usado se o usuário for um administrador local. Observe que as credenciais devem ser estabelecidas para a máquina virtual associada por meio da opção **Nome do usuário do S.O. guest** e **Senha do S.O. guest** dentro da definição de tarefa de backup associada.
- A credencial de login do sistema deve ter as permissões do administrador local.

Requisitos do Kerberos

- A autenticação baseada no Kerberos pode ser ativada por meio de um arquivo de configuração no dispositivo IBM Spectrum Protect Plus. Esta configuração substituirá o protocolo NTLM padrão do Windows. Observe que o Kerberos não permite que contas de usuário local sejam usadas e é adequado apenas para ambientes nos quais todas as máquinas estão em um único domínio.
- Somente para autenticação baseada em Kerberos, a identidade do usuário deve ser especificada no formato `user:password@FQDN`. O usuário especificado deve ser capaz de autenticar usando a senha registrada para obter um chamado de concessão de chamado (TGT) do centro de distribuição de chaves (KDC) no domínio especificado pelo nome completo do domínio.
- A autenticação do Kerberos também requer que o clock skew entre o Controlador de Domínio e o dispositivo IBM Spectrum Protect Plus seja menor que 5 minutos. Observe que o protocolo NTLM padrão do Windows não é dependente de tempo.

Requisitos do Linux

Sistemas Operacionais Suportados	<ul style="list-style-type: none">• Níveis de manutenção e de modificação do Red Hat Enterprise Linux 6.4 e mais recentes• Níveis de manutenção e de modificação do CentOS 6.4 e mais recentes• Níveis de manutenção e de modificação do Red Hat Enterprise Linux 7.0 e mais recentes• Níveis de manutenção e de modificação do CentOS 7.0 e mais recentes• Níveis de manutenção e de modificação do SUSE Linux Enterprise Server 12.0 e mais recentes
Sistemas de Arquivos Suportados	<ul style="list-style-type: none">• ext2• ext3• ext4• XFS

- Um sistema de arquivos criado em uma versão mais recente do kernel pode não ser montável em um sistema com um kernel mais antigo, nesse caso, a restauração de arquivos do sistema mais recente para o sistema mais antigo não é suportada.

O IBM Spectrum Protect Plus suporta apenas os sistemas operacionais disponíveis para seus hypervisors. Revise a documentação do hypervisor para obter informações sobre sistemas operacionais suportados.

Nota: O IBM Spectrum Protect Plus pode proteger e restaurar máquinas virtuais com outros sistemas de arquivos, mas somente os sistemas de arquivos listados anteriormente são elegíveis para indexação e restauração de arquivo.

- Quando a indexação de arquivo é executada em um ambiente Linux, os diretórios a seguir no recurso são ignorados:

```
/tmp  
/usr/bin  
/Drivers  
/bin  
/sbin
```

- Os arquivos em sistemas de arquivos virtuais como /proc, /sys e /dev também são ignorados. Os arquivos dentro desses diretórios não são incluídos no inventário do IBM Spectrum Protect Plus e não estão disponíveis para recuperação de arquivo.

Requisitos de Espaço

- O disco do sistema deve ter espaço temporário suficiente para salvar os resultados de indexação de arquivo.
- Quando os sistemas de arquivos são indexados, os arquivos de metadados temporários são gerados sob o diretório /tmp e, em seguida, excluídos assim que a indexação é concluída. A quantidade de espaço livre necessário para os metadados depende do número total de arquivos presentes no sistema. Certifique-se de que haja aproximadamente 350 MB de espaço livre por 1 milhão de arquivos.

Requisitos de software

- O Python versão 2.6 (qualquer nível) ou 2.7 (qualquer nível) deve ser instalado.

- Somente Red Hat Enterprise Linux/CentOS 6.x: Assegure-se de que O pacote `util-linux-ng` esteja atualizado executando **yum update util-linux-ng**. Dependendo de sua versão ou distribuição, o pacote pode ser chamado `util-linux`.
- Se os dados residirem em volumes de LVM, assegure-se de que a versão do LVM seja 2.0.2.118 ou mais recente. Execute **lvm version** para verificar a versão e execute **yum update lvm2** para atualizar o pacote, se necessário.
- Se os dados residirem em volumes LVM, o serviço **lvm2-lvmetad** deverá ser desativado, pois ele pode interferir na capacidade do IBM Spectrum Protect Plus de montar e assinar novamente as capturas instantâneas ou clones do grupo de volumes. Para desativar o serviço, conclua as seguintes etapas:

1. Execute os seguintes comandos:

```
systemctl stop lvm2-lvmetad
systemctl disable lvm2-lvmetad
```

2. Edite `/etc/lvm/lvm.conf` e especifique a configuração a seguir:

```
use_lvmetad = 0
```

Para obter detalhes sobre o serviço **lvmetad**, consulte [O Daemon de Metadados \(lvmetad\)](#).

- Se os dados residirem nos sistemas de arquivos XFS e a versão de **xfspgrog** estiver entre 3.2.0 e 4.1.9, a restauração do arquivo poderá falhar devido a um problema conhecido em **xfspgrog** que causa dano a um sistema de arquivos de clone ou de captura instantânea quando seu UUID é modificado. Para resolver esse problema, atualize **xfspgrog** para a versão 4.2.0 ou acima.

Para obter mais informações, consulte [Logs de relatório de erros do Debian](#).

Requisitos de Conectividade

O serviço SSH deve estar em execução na porta 22 no servidor e todos os firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor por meio de SSH. O subsistema SFTP para SSH também deve estar ativado.

Requisitos de autenticação e de privilégio

As credenciais especificadas para a máquina virtual devem especificar um usuário que tenha os privilégios **sudo** a seguir:

- A configuração `sudoers` deve permitir que o usuário execute comandos sem uma senha.
- A configuração `!requiretty` deve ser configurada.

A abordagem recomendada é criar um usuário do agente do IBM Spectrum Protect Plus dedicado com os privilégios a seguir. Configuração de amostra:

- Criar usuário: `useradd -m sppagent`

em que **sppagent** especifica o usuário do agente do IBM Spectrum Protect Plus.

- Configurar uma senha: `passwd <sppagent>`

Coloque as linhas a seguir no final de seu arquivo de configuração `sudoers`, geralmente `/etc/sudoers`. Se o arquivo `sudoers` existente estiver configurado para importar configurações de outro diretório (por exemplo, `/etc/sudoers.d`), também será possível colocar as linhas em um novo arquivo nesse diretório:

```
Defaults: sppagent !requiretty
sppagent ALL = (root) NOPASSWD:ALL
```

Microsoft Requisitos do Exchange Server

Antes de instalar o IBM Spectrum Protect Plus, revise os requisitos de hardware e software para o produto e outros componentes.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um

ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

Os requisitos de backup e restauração do banco de dados Exchange para o IBM Spectrum Protect Plus são os seguintes.

Configuração

Certifique-se de que a versão do Microsoft Exchange Server que está sendo usada seja suportada em seu sistema operacional.

Versões do Aplicativo

- Microsoft Exchange Server 2013 CU16 e níveis de CU e de manutenção mais recentes: Standard ou Enterprise editions.
- Microsoft Exchange Server 2016 CU 5 e níveis de CU e de manutenção mais recentes: Standard e Enterprise editions.
- Microsoft Exchange Server 2019 e níveis de manutenção mais recentes: Standard e Enterprise editions.

Nota: Os grupos de disponibilidade do banco de dados (DAG) do Microsoft Exchange são suportados.

Sistemas Operacionais

- Windows Server 2012R2 e níveis de manutenção mais recentes (kernel de 64 bits): Standard e Datacenter editions
- Windows Server 2016 e níveis de manutenção mais recentes (kernel de 64 bits): Standard e Datacenter editions
- Windows Server 2019 e níveis de manutenção mais recentes (kernel de 64 bits): Standard e Datacenter editions

Nota: A instalação do Windows Server 2019 Core é suportada. No entanto, o recurso de restauração granular não é suportado em uma instalação principal.

Notas Adicionais

Instale as correções e atualizações mais recentes do Microsoft Exchange Server em seu ambiente.

Para obter informações sobre o suporte de virtualização para o Exchange Server, consulte o [“Pré-requisitos para o Servidor Microsoft Exchange”](#) na página 161.

Software

Assegure-se de que uma versão suportada de um sistema operacional Windows de 64 bits esteja instalada.

Os pré-requisitos a seguir da Microsoft são necessários e devem ser instalados antes do uso do IBM Spectrum Protect Plus:

- Windows PowerShell 4 ou posterior
- Windows Management Framework 4 ou posterior

Ao usar o Microsoft Exchange Server 2013 e o recurso de restauração granular, o nível mínimo suportado para o Microsoft Exchange Messaging API (MAPI) Client and Collaboration Data Objects (MAPI/CDO) é a versão 6.5.8320.0.

Nota: O MAPI/CDO é necessário apenas para o Microsoft Exchange Server 2013. Isso não é necessário se você estiver executando o Microsoft Exchange Server 2016 ou o Exchange Server 2019.

Ao usar o recurso de restauração granular com o Microsoft Exchange Server 2016 ou com o Microsoft Exchange Server 2019, o Microsoft 32-bit Outlook 2016 ou o Microsoft 32-bit Outlook 2019 é necessário.

Os pré-requisitos a seguir da Microsoft são necessários e instalados automaticamente pelo recurso de restauração granular do IBM Spectrum Protect Plus, se ainda não estiverem presentes em sua máquina virtual.

- Pacote Redistribuível do Microsoft Visual C++ 2012 de 32 bits
- Pacote Redistribuível do Microsoft Visual C++ 2012 de 64 bits
- Pacote Redistribuível do Microsoft Visual C++ 2017 de 32 bits
- Pacote Redistribuível do Microsoft Visual C++ 2017 de 64 bits
- Microsoft .NET Framework 4.5
- Microsoft ReportViewer 2012 SP1 Redistribuível
- Tipos CLR do Sistema Microsoft SQL Server 2012
- Tipos CLR do Sistema Microsoft SQL Server 2014
- Tipos CLR do Sistema Microsoft SQL Server 2016

Dica: A instalação desses pré-requisitos pode requerer uma reinicialização do sistema. Para evitar uma reinicialização do sistema, assegure-se de que esses pré-requisitos estejam instalados antes de iniciar o recurso de restauração granular do IBM Spectrum Protect Plus.

Privilégios

Os usuários do agente IBM Spectrum Protect Plus têm os privilégios a seguir:

O Microsoft Exchange Server é protegido por autenticação baseada em função. Para que o agente do Microsoft Exchange funcione no ambiente IBM Spectrum Protect Plus, deve-se configurar os privilégios apropriados. Para obter mais informações, consulte [“Privilégios”](#) na página 161.

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus. As portas que são indicadas com "Aceitar" na coluna Regra de firewall usam conexões seguras (HTTPS ou SSL).

Tabela 9. Conexões de firewall do agente IBM Spectrum Protect Plus recebidas

Porta	Protocolo	Regra de firewall	Serviço	Descrição
5985	TCP	Aceitar	WinRM	Windows Serviço de Gerenciamento Remoto
5986	TCP	Aceitar	WinRM	Serviço de Gerenciamento Remoto do Secure Windows

Tabela 10. Conexões de firewall do agente IBM Spectrum Protect Plus de saída

Porta	Protocolo	Serviço	Descrição
3260*	TCP	iSCSI vSnap	Porta de destino do iSCSI vSnap usada para montar o LUNS para backup e recuperação

Tabela 10. Conexões de firewall do agente IBM Spectrum Protect Plus de saída (continuação)

Porta	Protocolo	Serviço	Descrição
137	UDP	vSnap SMB/CIFS	Porta de destino do vSnap SMB ou CIFS usada para montar compartilhamentos do sistema de arquivos para backup e recuperação do log de transações
138	UDP	vSnap SMB/CIFS	Porta de destino do vSnap SMB ou CIFS usada para montar compartilhamentos do sistema de arquivos para backup e recuperação do log de transações
139	TCP	vSnap SMB/CIFS	Porta de destino do vSnap SMB ou CIFS usada para montar compartilhamentos do sistema de arquivos para backup e recuperação do log de transações
445	TCP	vSnap SMB/CIFS	Porta de destino do vSnap SMB ou CIFS usada para montar compartilhamentos do sistema de arquivos para backup e recuperação do log de transações

*O inicializador iSCSI é necessário nesse nó.

Hardware

System	Espaço em Disco	Espaço em Disco para Operações de Restauração Granular
x64: hardware compatível suportado pelo sistema operacional e pelo Microsoft Exchange Server	Um mínimo de 200 MB de espaço em disco para o produto a ser instalado	Pelo menos 2,1 GB de espaço em disco para "Pré-requisitos adicionais da Microsoft", que serão instalados automaticamente se eles ainda não estiverem

Requisitos do Db2

Antes de registrar o Db2 com o IBM Spectrum Protect Plus, assegure-se de que seu ambiente atenda aos requisitos descritos.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

Os requisitos de backup e restauração do banco de dados IBM Db2 para IBM Spectrum Protect Plus são os seguintes.

Requisitos de configuração

Os bancos de dados IBM Db2 a seguir são suportados:

- Níveis de manutenção e níveis de modificação do IBM Db2 Versão 10.5 e mais recente: Enterprise Server Edition.
- Níveis de manutenção e níveis de modificação do IBM Db2 Versão 11.1 e mais recente: Enterprise Server Edition.

Sistemas Operacionais

Os seguintes sistemas operacionais são suportados:

- No PowerPC:
 - Níveis de modificação e de fix pack do AIX 7.1 e mais recentes (kernel de 64 bits).
 - Níveis de modificação e de fix pack do AIX 7.2 e mais recentes (kernel de 64 bits).
- No Linux x86_x64:
 - Níveis de manutenção e níveis de modificação do Red Hat Enterprise Linux 6.8 e mais recentes.
 - Níveis de manutenção e níveis de modificação do Red Hat Enterprise Linux 7 e mais recentes.
 - Níveis de manutenção e níveis de modificação do SUSE Linux Enterprise Server 11.0 SP4 e mais recentes.
 - Níveis de manutenção e níveis de modificação do SUSE Linux Enterprise Server 12.0 SP1 e mais recentes.
- No Linux on Power System (little endian)
 - Níveis de manutenção e de modificação do Red Hat Enterprise Linux 7.1 e mais recentes.
 - Níveis de manutenção e de modificação do SUSE Linux Enterprise Server 12.0 SP1 e mais recentes.

Notas adicionais

Instale as correções e atualizações mais recentes do IBM Db2 em seu ambiente.

O IBM Db2pureScale não é suportado

Certifique-se de que seu ambiente Db2 esteja configurado para atender aos seguintes critérios:

- A criação de log de archive do Db2 está ativada e o Db2 está no modo recuperável.
- Os volumes lógicos que retêm espaços de tabela do Db2 (dados e espaços de tabela temporários), o diretório do banco de dados local e os arquivos de log do Db2 são gerenciados pelo Logical Volume Manager (LVM2) no Linux e por JFS2 no AIX, respectivamente. LVM2 on Linux e JFS2 on AIX são usados para criar capturas instantâneas de volume provisório. O volume lógico cresce em tamanho com dados conforme muda no volume de origem, enquanto a captura instantânea existir. Para obter mais informações, consulte [“LVM2 e JFS2” na página 140](#).
- O Db2 deve estar no modo de backup paralelo se múltiplas partições devem ser protegidas. O modo de backup paralelo pode ser ativado usando as variáveis de registro do Db2. Para obter mais informações, consulte [“Pré-requisitos para o Db2” na página 137](#).

Software

Revise os requisitos de software a seguir:

- Os pacotes bash e sudo devem ser instalados. O sudo deve estar na versão 1.7.6p2 ou superior. Executar `sudo -V` para verificar a versão.

Nota: Os pacotes bash e sudo necessários são incluídos nos sistemas operacionais Linux86_64 e Linux Power Systems (little endian) suportados.

- O Python versão 2.6 (qualquer nível) ou 2.7 (qualquer nível) deve ser instalado no Linux.
- O Python versão 2.7.x deve ser instalado no AIX.
- Assegure-se de que a versão suportada do Linux x86_64, Linux Power Systems (little endian) ou AIX esteja instalada.

Conectividade

Certifique-se de que os seguintes critérios de conectividade estejam em vigor:

- O serviço SSH está em execução na porta 22 no servidor.
- Os firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor usando SSH.
- O subsistema SFTP para SSH está ativado.
- O servidor pode ser registrado usando um nome de DNS ou endereço IP. Os nomes de DNS devem ser resolvidos por IBM Spectrum Protect Plus.
- No AIX, assegure-se de que a comunicação NFS esteja configurada com portas reservadas, usando o comando: `nfs -p -o nfs_use_reserved_port=1`.

Autenticação e Privilégios

O servidor Db2 deve ser registrado no IBM Spectrum Protect Plus usando um usuário do sistema operacional que exista no servidor Db2 (referido como usuário do agente do IBM Spectrum Protect Plus).

Assegure-se de que a senha esteja configurada corretamente e que o usuário possa efetuar login sem receber outros avisos, como avisos para reconfigurar a senha.

O usuário do agente IBM Spectrum Protect Plus deve ter os seguintes privilégios:

- Privilégios para executar comandos como o usuário raiz e como o usuário do proprietário do software Db2 usando sudo. O IBM Spectrum Protect Plus requer isso para várias tarefas, como descobrir layouts de armazenamento, montar e desmontar discos e gerenciar bancos de dados.
 - A configuração `sudoers` deve permitir que o usuário do agente do IBM Spectrum Protect Plus execute comandos sem uma senha.
 - A configuração `!requiretty` deve ser configurada.
- Privilégios para ler o inventário do Db2 usando `/usr/local/bin/db2ls`. O IBM Spectrum Protect Plus requer este privilégio para descobrir e coletar informações sobre instâncias e bancos de dados IBM Db2.

Portas

As seguintes portas são usadas por agentes IBM Spectrum Protect Plus. Portas que são marcadas como Aceitar usam uma conexão segura (HTTPS/SSL).

Tabela 11. Conexões de firewall do agente IBM Spectrum Protect Plus recebidas

Porta	Protocolo	Firewall	Serviço	Descrição
22	TCP	Aceitar	SSH	Usado para transferência de dados SSH para e a partir do servidor vSnap interno.

Tabela 12. Conexões de firewall do agente IBM Spectrum Protect Plus de saída

Porta	Protocolo	Serviço	Descrição
111	TCP	VSnap RPC Port Bind	Permite que os clientes descubram portas que os clientes Open Network Computing (ONC) requerem para se comunicar com servidores ONC.
2049	TCP	vSnap NFS	Usado para compartilhamento de arquivo NFS por meio do vSnap.
20048	TCP	vSnap Mount NFS	Monta sistemas de arquivos vSnap em clientes, como o proxy VADP, servidores de aplicativos e armazenamentos de dados de virtualização.

Requisitos do MongoDB

Antes de registrar o MongoDB com IBM Spectrum Protect Plus, assegure-se de que seu ambiente atenda aos requisitos descritos.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

Os requisitos de backup e restauração do banco de dados MongoDB para o IBM Spectrum Protect Plus são os seguintes.

Requisitos de configuração

As seguintes versões de banco de dados MongoDB são suportadas:

- Níveis de manutenção e níveis de modificação do MongoDB Versão 3.6 e mais recentes: Community Server e Enterprise Server Editions.
- Níveis de manutenção e níveis de modificação do MongoDB Versão 4.0 e mais recentes: Community Server e Enterprise Server Editions.

Sistemas Operacionais

Os seguintes sistemas operacionais são suportados:

- No Linux x86_x64:
 - Níveis de manutenção e níveis de modificação do Red Hat Enterprise Linux 6.8 e mais recente
 - Níveis de manutenção e níveis de modificação do CentOS 6.8 e mais recente
 - Níveis de manutenção e níveis de modificação do Red Hat Enterprise Linux 7 e mais recente
 - Níveis de manutenção e níveis de modificação do CentOS 7 e mais recente
 - Níveis de manutenção e níveis de modificação do SUSE Linux Enterprise Server 12.0 SP1 e mais recente

- No Linux Power Systems (little endian):
 - Níveis de manutenção e de modificação do Red Hat Enterprise Linux 7.1 e mais recente
 - Níveis de manutenção e de modificação do CentOS 7 e mais recente

Nota: no Linux Power Systems (little endian), somente a edição do servidor enterprise do MongoDB é suportada.

Notas adicionais

Para ajudar a otimizar o desempenho, instale as correções e atualizações mais recentes do MongoDB disponíveis para seu ambiente.

Certifique-se de que seu ambiente MongoDB esteja configurado para atender aos seguintes critérios:

- O MongoDB é configurado como uma instância ou conjunto de réplicas independente. As operações de backup de instâncias de cluster fragmentado do MongoDB não são suportadas. Um backup sempre inclui todos os bancos de dados na instância.
- A instância do MongoDB está configurada para usar o Mecanismo de Armazenamento do WiredTiger.
- O usuário no registro do servidor de aplicativos MongoDB no IBM Spectrum Protect Plus deve ser capaz de recuperar informações e status do servidor do banco de dados do administrador MongoDB.
- Volumes lógicos de caminhos de dados e de log do MongoDB são gerenciados pelo Gerenciador de Volume Lógico (LVM2) Linux. O LVM2 é usado para criar capturas instantâneas do volume temporário. Os arquivos de banco de dados e o diário devem estar localizados em um único volume. O volume lógico cresce em tamanho com dados conforme muda no volume de origem, enquanto a captura instantânea existir. Para obter mais informações, consulte [“Linux LVM2 ” na página 199](#).

Software

Revise os requisitos de software a seguir:

- O Python versão V2.6 (qualquer nível) ou V2.7 (qualquer nível) deve ser instalado.
- Quando o servidor de aplicativos MongoDB executar o RHEL 6 ou CentOS 6, assegure-se de que o pacote `openssl` esteja na versão 1.0.1e-57 ou acima. Execute `"yum update openssl"` para atualizar para esse requisito.
- Assegure-se de que a versão suportada do Linux x86_64 ou Linux Power Little Endian esteja instalada.

Conectividade

Certifique-se de que os seguintes critérios de conectividade estejam em vigor:

- O serviço SSH está em execução na porta 22 no servidor.
- Os firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor usando SSH.
- O subsistema SFTP para SSH está ativado.
- O servidor de aplicativos pode ser registrado no IBM Spectrum Protect Plus usando um nome de DNS ou um endereço IP. Os nomes de DNS devem ser resolvidos por IBM Spectrum Protect Plus.

Autenticação e Privilégios

O servidor MongoDB deve ser registrado no IBM Spectrum Protect Plus usando um usuário do sistema operacional que exista no servidor MongoDB (referido como *Usuário do agente do IBM Spectrum Protect Plus* para o restante deste tópico).

Assegure-se de que a senha esteja configurada corretamente e que o usuário possa efetuar login sem receber outros avisos, como avisos para reconfigurar a senha.

No MongoDB, a criptografia baseada em SSL e a autenticação baseada em certificado não são suportadas.

Em MongoDB Enterprise Server Editions, somente a criptografia no armazenamento é suportada.

O usuário do agente IBM Spectrum Protect Plus deve ter os seguintes privilégios:

- Privilégios para executar comandos como o usuário raiz e como o usuário do proprietário do software MongoDB usando sudo. O IBM Spectrum Protect Plus requer este privilégio para tarefas, como descobrir layouts de armazenamento, montar e desmontar discos e gerenciar bancos de dados.
 - A configuração sudoers deve permitir que o usuário do agente do IBM Spectrum Protect Plus execute comandos sem uma senha.
 - A configuração !requiretty deve ser configurada.
- Privilégios para executar o módulo do servidor padrão MongoDB /usr/local/bin/mongodb. O IBM Spectrum Protect Plus requer esse privilégio para usar a API pymongo para se conectar aos servidores MongoDB usando o nome e a porta de DNS/IP designados da instância. Este mecanismo é usado para reunir informações sobre instâncias e bancos de dados MongoDB.
- Se o servidor MongoDB for protegido por autenticação baseada em função, para que o agente do MongoDB funcione no ambiente IBM Spectrum Protect Plus, deve-se configurar os privilégios apropriados. Para obter mais informações, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297.](#)

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus. As portas que são indicadas com Aceitar na coluna Regra de firewall usam conexões seguras (HTTPS/SSL).

Tabela 13. Conexões de firewall do agente IBM Spectrum Protect Plus recebidas

Porta	Protocolo	Regra de firewall	Serviço	Descrição
22	TCP	Aceitar	SSH	Usado para transferência de dados SSH para e do servidor vSnap interno

Tabela 14. Conexões de firewall do agente IBM Spectrum Protect Plus de saída

Porta	Protocolo	Serviço	Descrição
111	TCP	vSnap RPC Port Bind	Permite que os clientes descubram portas que os clientes Open Network Computing (ONC) requerem para se comunicar com servidores ONC
2049	TCP	vSnap NFS	Usado para compartilhamento de arquivo NFS via vSnap
20048	TCP	vSnap Mount NFS	Monta os sistemas de arquivos vSnap em clientes, como o proxy VADP, servidores de aplicativos e armazenamentos de dados de virtualização

Requisitos do Oracle

Revise os requisitos de backup e restauração do banco de dados Oracle para o IBM Spectrum Protect Plus.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

Requisitos de configuração

Versões do banco de dados

- Oracle 11g R2
- Oracle 12c R1
- Oracle 12c R2
- Oracle 18c

Nota: Para bancos de dados de vários locatários no Oracle 12c e mais recente, o IBM Spectrum Protect Plus suporta a proteção e recuperação do banco de dados do contêiner, incluindo todos os bancos de dados plugáveis (PDBs) abaixo dele. A recuperação granular de PDBs específicos pode ser executada por meio da recuperação de Restauração de Disco Instantânea combinada com RMAN.

Sistemas Operacionais

- Níveis de manutenção e de modificação do AIX 6.1 TL9 e mais recentes
- Níveis de manutenção e de modificação do AIX 7.1 e mais recentes
- Níveis de manutenção e modificação do Red Hat Enterprise Linux/CentOS 6.5 e mais recente
- Níveis de manutenção e modificação do Red Hat Enterprise Linux/CentOS 7.0 e mais recente
- Níveis de manutenção e de modificação do SUSE Linux Enterprise Server 11.0 SP4 e mais recentes
- Níveis de manutenção e de modificação do SUSE Linux Enterprise Server 12.0 SP1 e mais recentes
- Níveis de manutenção e de modificação do SUSE Linux Enterprise Server 15.0 e mais recentes

Notas adicionais

- O Oracle DataGuard não é suportado.
- Os bancos de dados devem estar no modo ARCHIVELOG. O IBM Spectrum Protect Plus não pode proteger bancos de dados em execução no modo NOARCHIVELOG.
- As recuperações do banco de dados Real Application Cluster (RAC) não reconhecem o conjunto de servidores. O IBM Spectrum Protect Plus pode recuperar bancos de dados para um RAC, mas não para conjuntos de servidores específicos.
- Os bancos de dados RAC devem ser configurados de forma que o local do Arquivo de controle de captura instantânea do RMAN aponte para o armazenamento compartilhado que está acessível a todas as instâncias de cluster.
- Ao restaurar um banco de dados Oracle que foi configurado para multiencadeamento no momento do backup, o banco de dados restaurado não é multiencadeado. O banco de dados restaurado deve ser reconfigurado manualmente para usar multiencadeamento.

Software

- Os pacotes **bash** e **sudo** devem ser instalados. O **sudo** deve ser a versão 1.7.6p2 ou acima. Execute **sudo -V** para verificar a versão.
- O Python versão 2.6.x ou 2.7.x deve ser instalado.
- **Somente RHEL/CentOS 6.x:**

Assegure-se de que o pacote `util-linux-ng` esteja atualizado executando: **`yum update util-linux-ng`**.

Dependendo de sua versão ou distribuição, o pacote pode ser chamado `util-linux`.

Conectividade

- O serviço SSH deve estar em execução na porta 22 no servidor e quaisquer firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor usando SSH. O subsistema SFTP para SSH também deve estar ativado.
- O servidor pode ser registrado usando um nome DNS ou endereço IP. Os nomes de DNS devem ser resolvidos por IBM Spectrum Protect Plus.
- Se o DNS não está disponível, deve-se incluir o servidor no arquivo `/etc/hosts` no dispositivo IBM Spectrum Protect Plus usando a linha de comandos.
- Ao registrar nós do Oracle RAC, registre cada nó usando seu IP físico ou nome. Não use um nome virtual ou Single Client Access Name (SCAN).

Autenticação e Privilégios

- O servidor Oracle deve ser registrado no IBM Spectrum Protect Plus usando um usuário do sistema operacional que existe no servidor Oracle. De agora em diante, o usuário é referido como o usuário do agente do IBM Spectrum Protect Plus.
- Assegure-se de que a senha esteja configurada corretamente e de que o usuário possa efetuar login sem outros prompts, como prompts para reconfigurar a senha.

O usuário do agente IBM Spectrum Protect Plus deve ter os seguintes privilégios:

- Privilégios para executar comandos como raiz e como usuários proprietários de software do Oracle (por exemplo, `oracle`, `grid`) usando **`sudo`**. Esses privilégios são necessários para tarefas como descoberta de layouts de armazenamento, montagem e desmontagem de discos e gerenciamento de bancos de dados e ASM.
 - A configuração `sudoers` deve permitir que o usuário do agente IBM Spectrum Protect Plus execute comandos sem uma senha.
 - A configuração `!requiretty` deve ser configurada.
 - A configuração `ENV_KEEP` deve permitir que as variáveis de ambiente `ORACLE_HOME` e `ORACLE_SID` sejam retidas.
- Privilégios para ler o inventário do Oracle. Esses privilégios são necessários para tarefas como descoberta e coleta de informações sobre Oracle homes e bancos de dados.

Para conseguir isso, o usuário do agente do IBM Spectrum Protect Plus deve pertencer ao grupo de inventário do Oracle, geralmente denominado `oinstall`.

Para obter informações sobre como criar um novo usuário com privilégios necessários, consulte [“Configuração de amostra de um usuário do agente do IBM Spectrum Protect Plus”](#) na página 39

NFS

O servidor Oracle deve ter o cliente NFS nativo do Linux ou AIX instalado. O IBM Spectrum Protect Plus usa NFS para montar volumes de armazenamento para operações de backup e restauração.

Durante a restauração do banco de dados, o recurso Oracle Direct NFS é necessário. O IBM Spectrum Protect Plus ativa automaticamente o Direct NFS se ele ainda não estiver ativado.

Para que o Direct NFS funcione corretamente, o executável `<ORACLE_HOME>/bin/oradism` em cada Oracle home deve ser de propriedade de raiz e ter privilégios `setuid`. Isso é geralmente pré-configurado pelo instalador do Oracle, mas em determinados sistemas, o binário pode não ter os privilégios necessários. Para obter mais informações, consulte o documento [Database Startup Failed with Direct NFS](#) no website de suporte do Oracle.

Execute os seguintes comandos para configurar os privilégios corretos:

- `chown root:oinstall <ORACLE_HOME>/bin/oradism`
- `chmod 750 <ORACLE_HOME>/bin/oradism`

em que `oinstall` especifica o grupo que possui a instalação.

Descoberta de banco

O IBM Spectrum Protect Plus descobre instalações e bancos de dados Oracle examinando os arquivos `/etc/oraInst.loc` e `/etc/oratab`, bem como a lista de processos do Oracle em execução. Se os arquivos não estiverem presentes em seu local padrão, o utilitário "localizar" deverá ser instalado no sistema para que o IBM Spectrum Protect Plus possa procurar os arquivos.

O IBM Spectrum Protect Plus descobre bancos de dados e seus layouts de armazenamento conectando-se às instâncias em execução e consultando os locais de seus arquivos de dados, arquivos de log e assim por diante. Para que o IBM Spectrum Protect Plus descubra corretamente os bancos de dados durante as operações de catalogação e cópia, os bancos de dados devem estar no modo "MOUNTED," "READ ONLY" ou "READ WRITE". O IBM Spectrum Protect Plus não pode descobrir ou proteger instâncias de banco de dados que estão encerradas.

Bloquear rastreamento

O IBM Spectrum Protect Plus requer que o Oracle Block Change Tracking esteja ativado em bancos de dados protegidos para executar backups incrementais de forma eficiente. Se o Block Change Tracking ainda não estiver ativado, o IBM Spectrum Protect Plus o ativará automaticamente durante a tarefa de backup.

Para customizar o posicionamento do arquivo de Block Change Tracking, deve-se ativar manualmente o recurso Block Change Tracking antes de executar uma tarefa de backup associada. Se o recurso for ativado automaticamente pelo IBM Spectrum Protect Plus, as regras a seguir serão usadas para determinar o posicionamento do arquivo do Block Change Tracking:

- Se o parâmetro **db_create_file_dest** estiver configurado, o arquivo de Block Change Tracking será criado no local especificado por este parâmetro.
- Se o parâmetro **db_create_file_dest** não estiver configurado, o arquivo de Block Change Tracking será criado no mesmo diretório que o espaço de tabela SYSTEM.

Backup de log

- O daemon **cron** deve ser ativado no servidor de aplicativos.
- O usuário do agente do IBM Spectrum Protect Plus deve ter os privilégios necessários para usar o comando **crontab** e criar tarefas cron. Os privilégios podem ser concedidos por meio do arquivo de configuração `cron.allow`.

Configuração de amostra de um usuário do agente do IBM Spectrum Protect Plus

Os comandos abaixo são exemplos para criar e configurar um usuário do sistema operacional que será usado pelo IBM Spectrum Protect Plus para efetuar login no servidor Oracle. A sintaxe de comando pode variar de acordo com seu tipo e versão de sistema operacional.

- Crie o usuário que será designado como o usuário do agente IBM Spectrum Protect Plus: `useradd -m sppagent`
- Configure uma senha: `passwd sppagent`

- Se estiver usando a autenticação baseada em chave, coloque a chave pública no diretório /home/sppagent/.ssh/authorized_keys ou no arquivo apropriado, dependendo de sua configuração do SSHD, e assegure-se de que a propriedade e as permissões corretas estejam configuradas, tal como:

```
chown -R sppagent:sppagent /home/sppagent/.ssh
chmod 700 /home/sppagent/.ssh
chmod 600 /home/sppagent/.ssh/authorized_keys
```

- Inclua o usuário na instalação do Oracle e no grupo OSDBA: `usermod -a -G oinstall, dba sppagent`
- Se o ASM estiver em uso, inclua também o usuário no grupo OSASM: `usermod -a -G asmadmin sppagent`
- Coloque as linhas a seguir no final de seu arquivo de configuração sudoers, geralmente /etc/sudoers. Se o arquivo sudoers existente estiver configurado para importar a configuração de outro diretório (por exemplo, /etc/sudoers.d), também será possível colocar as linhas em um novo arquivo nesse diretório:

```
Defaults:sppagent! requiretty
Defaults:sppagent env_keep + = "ORACLE_HOME "
Defaults:sppagent env_keep+= "ORACLE_SID"
sppagent ALL = (ALL) NOPASSWD:ALL
```

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus. As portas que são indicadas com "Aceitar" na coluna Regra de firewall usam uma conexão segura (HTTPS ou SSL).

Tabela 15. Conexões de firewall do agente IBM Spectrum Protect Plus recebidas

Porta	Protocolo	Regra de firewall	Serviço	Descrição
22	TCP	Aceitar	SSH	Usado para transferência de dados SSH para e a partir do servidor vSnap interno.

Tabela 16. Conexões de firewall do agente IBM Spectrum Protect Plus de saída

Porta	Protocolo	Serviço	Descrição
111	TCP	VSnap RPC Port Bind	Permite que os clientes descubram portas que os clientes Open Network Computing (ONC) requerem para se comunicar com servidores ONC.
443	TCP	HTTPS	Permite que o servidor Oracle se comunique com o IBM Spectrum Protect Plus para enviar alertas em caso de falhas de backup de log.

Tabela 16. Conexões de firewall do agente IBM Spectrum Protect Plus de saída (continuação)

Porta	Protocolo	Serviço	Descrição
2049	TCP	vSnap NFS	Usado para compartilhamento de arquivo NFS por meio do vSnap.
20048	TCP	vSnap Mount NFS	Monta sistemas de arquivos vSnap em clientes como o Proxy VADP, os servidores de aplicativos e os armazenamentos de dados de virtualização.

Microsoft Requisitos do SQL Server

Revise os requisitos de backup e restauração do banco de dados Microsoft SQL Server para o IBM Spectrum Protect Plus.

Para ajudar a assegurar que as operações de backup e restauração sejam executadas com sucesso, seu sistema deve atender aos requisitos de hardware e de software. Use os seguintes requisitos como um ponto de início. Para obter os requisitos mais atuais, que podem incluir atualizações, consulte a [nota técnica 2013790](#).

Configuração

Versões do banco de dados

- SQL Server 2008 R2 SP3
- SQL Server 2012
- SQL Server 2012 SP2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

Para obter o melhor desempenho, instale as correções e atualizações mais recentes do SQL Server em seu ambiente.

Sistemas operacionais

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

O Windows Remote Shell (WinRM) deve estar ativado.

Uma rota iSCSI deve ser ativada entre o sistema SQL Server e o servidor vSnap. Para obter mais informações, consulte [Microsoft iSCSI Initiator Step-by-Step Guide](#).

As tarefas de inventário do IBM Spectrum Protect Plus descobrem bancos de dados do sistema e marcam os bancos de dados que são elegíveis para proteção. Os backups de log são marcados como inelegíveis para todos os bancos de dados do sistema e bancos de dados em execução no modelo de recuperação simples.

OLTP na memória

O processamento de transações on-line (OLTP) na memória é um mecanismo de banco de dados otimizado na memória que é usado para melhorar o desempenho do aplicativo de banco de dados. Esse mecanismo é suportado no SQL Server 2014 e mais recente. Os requisitos e limitações a seguir se aplicam ao uso do OLTP na Memória:

- O caminho máximo do arquivo de restauração deve ter menos de 256 caracteres. Se o caminho original exceder esse comprimento, considere usar um caminho de arquivo de restauração customizado para reduzir o comprimento.
- Os metadados que podem ser restaurados estão sujeitos aos recursos de restauração do Volume Shadow Copy Service (VSS) e do SQL Server.

Backup incremental

O IBM Spectrum Protect Plus usa a tecnologia de diário de mudanças de número de sequência de atualização (USN) para executar backups incrementais em um ambiente do SQL Server. O diário de mudança USN fornece rastreamento de intervalo de gravação para um volume quando o tamanho do arquivo atende ao requisito de limite mínimo de tamanho de arquivo. As informações de deslocamento de bytes mudados e de extensão de comprimento podem ser consultadas em um arquivo específico.

Os seguintes requisitos ativam o rastreamento de intervalo de gravação:

- Windows Server 2012 R2 ou mais recente
- NTFS versão 3.0 ou posterior

As seguintes tecnologias não são suportadas para rastreamento de bytes mudados:

- Resilient File System (ReFS)
- Protocolo de Bloco de Mensagens do Servidor (SMB) 3.0
- SMB TFO (Failover Transparente)
- SMB 3.0 com compartilhamentos de arquivos de scale-out (SO)

Por padrão, 512 MB de espaço são alocados para registro no diário de mudança de USN. Além disso, quando o estouro de diário for detectado, um tamanho de diário de 2 GB será alocado para gerenciar o sistema de arquivos ocupado.

O espaço mínimo necessário para o armazenamento de cópia de sombra é de 100 MB, embora mais espaço possa ser necessário em sistemas com maior atividade. O agente do SQL Server verificará o espaço do volume de origem e fará com que um backup falhe se o espaço livre no volume de origem for menor que 100 MB. Uma mensagem de aviso é exibida no log da tarefa quando o espaço livre é menor que 10% e, em seguida, o backup continua.

Um backup de base é forçado quando as seguintes condições são detectadas:

- A descontinuidade do diário é relatada devido ao log atingir o tamanho máximo, à desativação do registro no diário ou mudando o ID de USN catalogado.
- O tamanho do arquivo é menor ou igual ao tamanho do limite controlado, que, por padrão, é 1 MB .
- Um arquivo é incluído após uma tarefa de backup anterior.

Backup de log

Antes de copiar arquivos de log para o repositório do vSnap, o IBM Spectrum Protect Plus usa a pasta de backup que é configurada para a instância do SQL server para montar a coleção de logs. Um espaço livre suficiente deve estar disponível para armazenar logs de transações entre as tarefas de backup. A área de preparação pode ser modificada mudando a configuração da pasta de backup usando o SQL Server Management Studio (SSMS).

Para assegurar que o Backup do log do SQL Server funcione adequadamente, uma mudança de Política de Grupo do Windows pode ser necessária.

A configuração do Objeto de Política de Grupo (GPO) para a política **Segurança de rede: Nível de autenticação do LAN Manager**, localizada em **Configuração do computador > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança**, deve ser configurada para uma das opções a seguir:

- **Não Definido**
- **Enviar apenas resposta NTLMv2**
- **Envie apenas a resposta NTLMv2. Refuse LM**
- **Envie apenas a resposta NTLMv2. Refuse LM & NTLM**

A opção **Enviar somente resposta do NTLM** não é compatível com a versão do vSnap CIFS ou SMB e pode causar problemas de autenticação do CIFS.

Configurando grupos de disponibilidade do SQL Server AlwaysOn

Configure a instância preferencial para operações de backup usando o SQL Server Management Studio. Execute as seguintes etapas:

1. Selecione o nó do **Grupo de disponibilidade**.
2. Selecione o grupo de disponibilidade que você deseja configurar e, em seguida, selecione **Propriedades**.
3. Na caixa de diálogo **Propriedades do grupo de disponibilidade**, selecione **Preferências de backup**.

Selecione qualquer opção na área de janela **Onde os backups devem ocorrer**. Quando a réplica secundária for preferencial e mais de uma réplica secundária estiver disponível, o executor de tarefa do IBM Spectrum Protect Plus O executor de tarefa selecionará a primeira réplica secundária na lista preferencial que é relatada pelo agente do SQL Server IBM Spectrum Protect Plus .

O agente SQL Server configura o tipo de backup do VSS como COPY_ONLY.

Registro e autenticação

Registre cada servidor SQL com o IBM Spectrum Protect Plus por nome ou endereço IP. Ao registrar um nó do Cluster SQL Server (AlwaysOn), registre cada nó por nome ou endereço IP. Os endereços IP devem ser voltados ao público e devem atender na porta 5985. O nome completo do domínio deve ser resolvível e roteável a partir do dispositivo IBM Spectrum Protect Plus.

A identidade do usuário deve ter direitos suficientes para instalar e iniciar o Serviço de Ferramentas do IBM Spectrum Protect Plus no nó, incluindo os direitos de **Efetuar logon como um serviço**. Para obter mais informações, consulte o artigo [Incluir o direito Efetuar logon como um serviço em uma conta no website da Microsoft](#).

A identidade do usuário seguirá o formato padrão *domain\Name* se a máquina virtual estiver conectada a um domínio. O formato *local administrator* será usado se o usuário for um administrador local.

Kerberos

A autenticação baseada em Kerberos pode ser ativada especificando um arquivo de configuração no dispositivo IBM Spectrum Protect Plus. As configurações substituirão o protocolo Windows NTLM padrão.

Somente para autenticação baseada em Kerberos, a identidade do usuário deve ser especificada no formato `username@FQDN`. O nome do usuário deve ser capaz de autenticar-se usando a senha registrada para obter um chamado de concessão de chamado (TGT) do centro de distribuição de chaves (KDC) no domínio especificado pelo nome completo do domínio.

Privilégios

O usuário do agente IBM Spectrum Protect Plus de um SQL server deve ter as permissões a seguir:

- Permissões do `public` e `sysadmin` do SQL Server

- Permissão de administração local do Windows, que é requerida pela estrutura VSS, e acesso de volume e disco
- Permissões para acessar recursos de cluster em um ambiente do SQL Server AlwaysOn e SQL Server FCI.

Cada instância do SQL Server pode usar uma conta do usuário específica para acessar os recursos dessa instância do SQL Server.

A estrutura baseada em VDI do SQL Server é usada para interagir com os bancos de dados SQL Server e para registrar operações de backup e de restauração. Uma conexão VDI requer permissões do sysadmin do SQL Server. O proprietário de um banco de dados restaurado não muda para o proprietário original. Uma etapa manual é necessária para modificar o proprietário de um banco de dados restaurado. Para obter mais informações sobre a estrutura VDI, consulte o artigo da Microsoft a seguir: [As operações de backup e restauração de VDI do SQL Server requerem privilégios Sysadmin.](#)

A conta de serviço do SQL Server de destino deve ter permissões para acessar os arquivos de restauração do SQL Server. Consulte "Considerações administrativas" no artigo da Microsoft a seguir: [Protegendo Arquivos de Dados e de Log.](#)

O Planejador de Tarefas do Windows é usado para planejar backups do log. Dependendo do ambiente, os usuários podem receber o erro a seguir: Uma sessão de logon especificada não existe. Ela pode já ter sido finalizada. Esse erro é devido a uma configuração de Política de grupo de acesso à rede que precisa ser desativada. Para obter mais informações sobre como desativar esse GPO, consulte o artigo de Suporte da Microsoft a seguir: [Uma sessão de logon especificada não existe. Ela pode já ter sido finalizada. Erro quando você tenta mapear para uma unidade de rede de um compartilhamento DFS.](#)

Portas

As portas a seguir são usadas pelo Usuários do agente IBM Spectrum Protect Plus. As portas que são indicadas com "Aceitar" usam uma conexão segura (HTTPS ou SSL).

Tabela 17. Conexões de firewall do agente IBM Spectrum Protect Plus recebidas

Porta	Protocolo	Firewall	Serviço	Descrição
5985	TCP	Aceitar	WinRM	Windows Serviço de Gerenciamento Remoto
5986	TCP	Aceitar	WinRM	Serviço de Gerenciamento Remoto do Secure Windows

Tabela 18. Conexões de firewall do agente IBM Spectrum Protect Plus de saída

Porta	Protocolo	Serviço	Descrição
3260 O inicializador iSCSI é necessário nesse nó.	TCP	iSCSI vSnap	Porta de destino do vSnap iSCSI usada para montar LUNS para operações de backup e de recuperação.

Tabela 18. Conexões de firewall do agente IBM Spectrum Protect Plus de saída (continuação)

Porta	Protocolo	Serviço	Descrição
137	UDP	vSnap SMB/CIFS	Porta de destino SMB/CIFS do vSnap usada para montar compartilhamentos de sistemas de arquivos para operações de backup e recuperação do log de transações.
138	UDP	vSnap SMB/CIFS	Porta de destino SMB/CIFS do vSnap usada para montar compartilhamentos de sistemas de arquivos para operações de backup e recuperação do log de transações.
139	TCP	vSnap SMB/CIFS	Porta de destino SMB/CIFS do vSnap usada para montar compartilhamentos de sistemas de arquivos para operações de backup e recuperação do log de transações.
443	TCP	HTTPS	Permite que o SQL server se comunique com o IBM Spectrum Protect Plus para enviar alertas em caso de falhas de backup do log.
445	TCP	vSnap SMB/CIFS	Porta de destino do vSnap SMB/CIFS usada para montar compartilhamentos do sistema de arquivos para operações de backup e recuperação do log de transações.

Obtendo o pacote de instalação do IBM Spectrum Protect Plus

É possível obter o pacote de instalação do IBM Spectrum Protect Plus a partir de um site de download da IBM, como o Passport Advantage ou Fix Central. Esses pacotes contêm arquivos que são necessários para instalar ou atualizar os componentes do IBM Spectrum Protect Plus.

Antes de Iniciar

Para obter a lista de pacotes de instalação por componente, e os links para o site de download para os arquivos, consulte [nota técnica 879861](#).

Procedimento

Faça download do arquivo de instalação apropriado.

Um arquivo de instalação diferente é fornecido para instalação em sistemas VMware e Microsoft Hyper-V. Assegure-se de fazer download do arquivo correto para seu ambiente.

Importante: Não mude os nomes dos arquivos de instalação ou de atualização. Os nomes de arquivos originais são necessários para que o processo de instalação ou de atualização seja concluído sem erros.

Conceitos relacionados

[“Atualizando componentes do IBM Spectrum Protect Plus” na página 83](#)

É possível atualizar o dispositivo virtual IBM Spectrum Protect Plus, servidores vSnap e os servidores proxy VADP para obter os recursos e aprimoramentos mais recentes. As correções e atualizações de software são instaladas usando o console administrativo do IBM Spectrum Protect Plus ou a interface da linha de comandos para esses componentes.

Tarefas relacionadas

[“Instalando o IBM Spectrum Protect Plus como um dispositivo virtual VMware” na página 46](#)

Para instalar o IBM Spectrum Protect Plus em um ambiente VMware, implemente um modelo Open Virtualization Format (OVF). A implementação de um modelo OVF cria um dispositivo virtual que contém o aplicativo em um host VMware, como um servidor ESXi.

[“Instalando o IBM Spectrum Protect Plus como um dispositivo virtual Hyper-V” na página 48](#)

Para instalar o IBM Spectrum Protect Plus em um ambiente do Microsoft Hyper-V, importe o modelo IBM Spectrum Protect Plus for Hyper-V. A importação de um modelo cria um dispositivo virtual que contém o aplicativo IBM Spectrum Protect Plus em uma máquina virtual Hyper-V. Um servidor vSnap local que já está nomeado e registrado também é instalado no dispositivo virtual.

[“Instalando servidores vSnap” na página 53](#)

Ao implementar um dispositivo IBM Spectrum Protect Plus, um servidor vSnap é instalado automaticamente. Este servidor é o destino do backup primário. Em ambientes corporativos maiores, podem ser necessários servidores vSnap adicionais.

Instalando o IBM Spectrum Protect Plus como um dispositivo virtual VMware

Para instalar o IBM Spectrum Protect Plus em um ambiente VMware, implemente um modelo Open Virtualization Format (OVF). A implementação de um modelo OVF cria um dispositivo virtual que contém o aplicativo em um host VMware, como um servidor ESXi.

Antes de Iniciar

Execute as seguintes tarefas:

- Revise os requisitos do sistema IBM Spectrum Protect Plus em [“Requisitos do Componente” na página 11](#) e [“Requisitos do Hypervisor” na página 23](#).
- Faça download do arquivo de instalação do modelo de dispositivo virtual CC1QCML . ova por meio do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [nota técnica 879861](#).
- Verifique a soma de verificação MD5 do arquivo de instalação do modelo transferido por download. Certifique-se de que a soma de verificação gerada corresponda à fornecida no arquivo de Soma de verificação MD5, que faz parte do download do software.
- Durante a implementação, será solicitado que insira propriedades de rede a partir da interface com o usuário do VMware. É possível inserir uma configuração de endereço IP estático, ou deixar todos os campos em branco para usar uma configuração DHCP.
- Para redesignar um endereço IP estático após a implementação, é possível usar a ferramenta NetworkManager Text User Interface (nmtui). Para obter mais informações, consulte [“Designando um endereço IP estático” na página 50](#).

Observe as seguintes considerações:

- Pode ser necessário configurar um conjunto de endereços IP que está associado à rede da MV na qual você planeja implementar o IBM Spectrum Protect Plus. A configuração correta do conjunto de endereços IP inclui a configuração do intervalo de endereço IP (se usada), máscara de rede, gateway, sequência de procura de DNS e um endereço IP do servidor DNS.
- Se o nome do host do dispositivo IBM Spectrum Protect Plus mudar após a implementação, por intervenção do usuário ou se um novo endereço IP for adquirido por meio do DNS, o dispositivo IBM Spectrum Protect Plus deverá ser reiniciado.
- Um gateway padrão deve ser configurado corretamente antes da implementação. Várias sequências de DNS são suportadas e devem ser separadas por vírgulas sem o uso de espaços.
- Para versões mais recentes do vSphere, o vSphere Web Client pode ser necessário para implementar dispositivos IBM Spectrum Protect Plus.
- O IBM Spectrum Protect Plus não foi testado para ambientes IPv6.

Procedimento

Para instalar o IBM Spectrum Protect Plus como um dispositivo virtual, conclua as seguintes etapas:

1. Implemente o IBM Spectrum Protect Plus executando uma das seguintes ações:
 - a) Se você estiver usando o vSphere Client, no menu **Ações**, clique em **Implementar modelo OVF**.
 - b) Se você estiver usando o vSphere Web Client, clique em **Criar/Registrar VM**, em seguida, selecione **Implementar uma máquina virtual por meio de um arquivo OVF ou OVA**.
2. Selecione um recurso ESXi para executar o dispositivo virtual. Clique em **Avançar**.
3. Detalhes da revisão. Clique em **Avançar**.

Importante:

Se você estiver usando o vSphere Web Client, verifique se `disk.enableUUID = true` é apresentado em **Configuração extra**. Se não for esse o caso ou se você estiver usando o vSphere Client, continue com as etapas de instalação e ative essa opção por meio do vSphere Web Client mais tarde.

4. Especifique o local do arquivo `CC1QCML.ova` e selecione-o. Clique em **Avançar**.
5. Forneça um nome significativo para o modelo, que se torna o nome de sua máquina virtual. Identifique um local apropriado para implementar a máquina virtual. Clique em **Avançar**.
6. Selecione o armazenamento para o qual o dispositivo virtual deve ser instalado. O armazenamento de dados desse armazenamento deve ser configurado com o host de destino. O arquivo de configuração do dispositivo virtual e os arquivos de disco virtual serão armazenados nele. Assegure-se de que o armazenamento seja grande o suficiente para acomodar o dispositivo virtual incluindo os arquivos de disco virtual associados a ele. Selecione um formato de disco dos discos virtuais. O thick provisioning permite melhor desempenho do dispositivo virtual. O thin provisioning usa menos espaço em disco em detrimento do desempenho. Clique em **Avançar**.
7. Leia os detalhes do modelo e aceite o Contrato de Licença do Usuário Final. Marque **Eu aceito todos os contratos de licença** para o vSphere Client ou clique em **Aceitar** para vSphere Web Client. Clique em **Avançar**.
8. Selecione redes para serem usadas pelo modelo implementado. Várias redes disponíveis no servidor ESXi podem estar disponíveis clicando em **Rede de destino**. Selecione uma rede de destino que permita definir a alocação do endereço IP apropriado para a implementação da máquina virtual. Clique em **Avançar**.
9. Para o vSphere Web Client, insira os valores de propriedade para o dispositivo virtual: DNS, Gateway padrão, Domínio, Endereço IP da rede e Prefixo de rede. Um endereço IP estático pode ser fornecido. Se deixado em branco, um endereço IP dinâmico designado por um servidor DHCP será usado. O prefixo de rede deve ser inserido usando a notação Classless Inter-Domain Routing (CIDR), em que os valores válidos são 1 - 24. Clique em **Avançar**.

Nota: Para o vSphere Client, essas propriedades podem ser configuradas usando a ferramenta NetworkManager Text User Interface (nmtui). Além disso, as informações para o campo Domínio de

procura podem ser incluídas usando esse comando. Para obter mais informações, consulte [Designando um endereço IP estático](#).

10. Revise suas configurações de modelo. Clique em **Concluir** para sair do assistente e iniciar a implementação do modelo OVF.
11. Após a implementação do modelo OVF, ligue a VM recém-criada. É possível ligar a VM a partir do vSphere Client.

Importante: Espere alguns minutos para que o IBM Spectrum Protect Plus seja totalmente inicializado.

O que Fazer Depois

Depois que o dispositivo virtual tiver sido implementado, o aplicativo IBM Spectrum Protect Plus, bem como um servidor vSnap local que é integrado a ele, será registrado e instalado nele automaticamente. Para iniciar o IBM Spectrum Protect Plus, conclua as ações a seguir:

Ação	Como
Conecte-se ao console do dispositivo virtual IBM Spectrum Protect Plus usando VMware Remote Console ou SSH. Defina as configurações de rede usando o NetworkManager Text User Interface (nmtui).	Consulte Designando um endereço IP estático .
Upload da chave do produto.	Consulte “Fazendo Upload da Chave do Produto” na página 50 .
Inicie IBM Spectrum Protect Plus a partir de um navegador da web suportado.	Consulte “Inicie o IBM Spectrum Protect Plus” na página 71 .

Instalando o IBM Spectrum Protect Plus como um dispositivo virtual Hyper-V

Para instalar o IBM Spectrum Protect Plus em um ambiente do Microsoft Hyper-V, importe o modelo IBM Spectrum Protect Plus for Hyper-V. A importação de um modelo cria um dispositivo virtual que contém o aplicativo IBM Spectrum Protect Plus em uma máquina virtual Hyper-V. Um servidor vSnap local que já está nomeado e registrado também é instalado no dispositivo virtual.

Antes de Iniciar

Execute as seguintes tarefas:

- Revise os requisitos do sistema IBM Spectrum Protect Plus em [“Requisitos do Componente” na página 11](#) e [“Requisitos do Hypervisor” na página 23](#).
- Faça download do arquivo de instalação CC1QDML.exe por meio do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [nota técnica 879861](#).
- Revise os requisitos adicionais do sistema Hyper-V. Consulte [Requisitos do sistema para Hyper-V no Windows Server](#).
- Verifique a soma de verificação MD5 do arquivo de instalação do modelo transferido por download. Certifique-se de que a soma de verificação gerada corresponda à fornecida no arquivo de Soma de verificação MD5, que faz parte do download do software.
- Se o nome do host do dispositivo virtual IBM Spectrum Protect Plus mudar após a implementação, por intervenção do usuário ou se um novo endereço IP for adquirido por meio de DNS, o dispositivo virtual IBM Spectrum Protect Plus deverá ser reiniciado.
- Todos os servidores Hyper-V, incluindo nós do cluster, devem ter o Microsoft iSCSI Initiator Service em execução em suas listas de Serviços. Configure o tipo de inicialização desse serviço como Automático para que ele inicie a execução quando o servidor for iniciado.

- Privilégios administrativos podem ser necessários para concluir determinadas etapas durante o processo de instalação.

Procedimento

Para instalar o IBM Spectrum Protect Plus como um dispositivo virtual, conclua as seguintes etapas:

1. Copie o arquivo CC1QDML . exe para o servidor Hyper-V.
2. Abra o instalador e conclua o Assistente de configuração.
3. Abra o Hyper-V Manager e selecione o servidor necessário.
4. Na área de janela **Ações** no Hyper-V Manager, clique em **Importar máquina virtual**. O assistente Importar máquina virtual é aberto. Clique em **Avançar**.
5. Na etapa **Localizar pasta**, clique em **Procurar...** e navegue para a pasta que foi designada durante a instalação. Selecione a pasta com **SPP-{release}** dentro dela. Clique em **Avançar**.
6. Na etapa **Selecionar máquina virtual**, assegure-se de que a máquina virtual **SPP-{release}** esteja selecionada e, em seguida, clique em **Avançar**. O diálogo **Escolher Tipo de Importação** é aberto.
7. Na etapa **Escolher tipo de importação**, selecione **Registrar a máquina virtual no local (usar o ID exclusivo existente)**. Clique em **Avançar**.
Importante: Não importe múltiplas alianças virtuais do IBM Spectrum Protect Plus em um único servidor Hyper-V.
8. Na etapa **Conectar rede**, configure a Conexão para o comutador virtual a ser usado. Clique em **Avançar**.
9. Na etapa **Resumo**, revise a Descrição. Clique em **Concluir** para fechar o assistente Importar máquina virtual.
10. No Hyper-V Manager, localize a nova máquina virtual denominada **SPP-{release}**. Clique com o botão direito nessa máquina virtual e clique em **Configurações**.
11. O diálogo Configurações para essa máquina virtual será aberto. Na área de janela esquerda, clique em **Hardware > Controlador IDE 0 > Unidade de disco rígido**.
12. Na seção Mídia, assegure-se de que o disco rígido virtual correto esteja selecionado. Anote o nome do arquivo do disco virtual original. Clique em **Editar (Edit)**.
13. O Assistente de edição de disco rígido virtual será aberto. Acesse a etapa **Escolher ação**.
14. Na etapa **Escolher ação**, clique em **Converter** e, em seguida, clique em **Avançar**.
15. Na etapa **Escolher formato de disco**, assegure-se de que **VHDX** esteja selecionado. Clique em **Avançar**.
16. Para a etapa **Escolher tipo de disco**, clique em **Tamanho fixo**. Clique em **Avançar**.
17. Para a etapa **Configurar disco**, localize a pasta para armazenar o arquivo de disco virtual do dispositivo virtual IBM Spectrum Protect Plus. Reutilize o mesmo nome de arquivo que foi indicado na Etapa 12. Se o mesmo diretório de instalação da Etapa 2 for reutilizado, use um nome diferente. Clique em **Avançar**.
Importante: Assegure-se de que a unidade de disco na qual a pasta reside tenha espaço em disco suficiente disponível para acomodar o arquivo de disco virtual de tamanho fixo.
18. Na etapa **Resumo**, revise a Descrição. Clique em **Concluir** para fechar o assistente Editar disco rígido virtual e para iniciar a conversão do disco virtual. Quando o processo for concluído, o arquivo de disco rígido virtual original poderá ser excluído.
19. No diálogo Configurações para a máquina virtual, clique em **Procurar**. Abra o arquivo de disco rígido virtual (VHDX) recém-criado que foi criado na etapa anterior.
20. Repita as etapas 12 a 19 para cada disco rígido em **Hardware > Controlador SCSI**. Clique em **OK** para fechar o diálogo Configurações.
21. No Hyper-V Manager, clique com o botão direito na máquina virtual e clique em **Iniciar**.
22. Use o Hyper-V Manager para identificar o endereço IP da nova máquina virtual, se o endereço for designado automaticamente. Para designar um IP estático à máquina virtual, use a ferramenta NetworkManager Text User Interface (nmtui).

Para obter mais informações, consulte [“Designando um endereço IP estático”](#) na página 50.

O que Fazer Depois

Depois de instalar o dispositivo virtual, conclua as seguintes ações:

Ação	Como
Reinicie o dispositivo virtual.	Consulte a documentação para o dispositivo virtual.
Upload da chave do produto.	Consulte “Fazendo Upload da Chave do Produto” na página 50.
Inicie IBM Spectrum Protect Plus a partir de um navegador da web suportado.	Consulte “Inicie o IBM Spectrum Protect Plus” na página 71.

Designando um endereço IP estático

Para redesignar um novo endereço IP estático após a implementação inicial, um administrador de rede pode designar um endereço IP estático usando a ferramenta NetworkManager Text User Interface (nmtui). São necessários privilégios de sudo para executar nmtui.

Procedimento

Para redesignar um novo endereço IP estático, certifique-se de que a máquina virtual do IBM Spectrum Protect Plus esteja ligada e conclua as seguintes etapas:

1. Efetue logon no console da máquina virtual com o ID do usuário **serveradmin**.
A senha inicial é sppDP758 .
2. A partir de uma linha de comandos do CentOS, insira nmtui para abrir a interface.
3. No menu principal, selecione **Editar uma conexão** e, em seguida, clique em **OK**.
4. Selecione a conexão de rede e, em seguida, clique em **Editar**.
5. Na tela **Editar conexão**, insira um endereço IP estático disponível que ainda não esteja em uso.
6. Salve a configuração de IP estático, clicando em **OK** e, em seguida, reinicie o dispositivo IBM Spectrum Protect Plus.

Tarefas relacionadas

[“Instalando o IBM Spectrum Protect Plus como um dispositivo virtual VMware”](#) na página 46

Para instalar o IBM Spectrum Protect Plus em um ambiente VMware, implemente um modelo Open Virtualization Format (OVF). A implementação de um modelo OVF cria um dispositivo virtual que contém o aplicativo em um host VMware, como um servidor ESXi.

[“Instalando o IBM Spectrum Protect Plus como um dispositivo virtual Hyper-V”](#) na página 48

Para instalar o IBM Spectrum Protect Plus em um ambiente do Microsoft Hyper-V, importe o modelo IBM Spectrum Protect Plus for Hyper-V. A importação de um modelo cria um dispositivo virtual que contém o aplicativo IBM Spectrum Protect Plus em uma máquina virtual Hyper-V. Um servidor vSnap local que já está nomeado e registrado também é instalado no dispositivo virtual.

Fazendo Upload da Chave do Produto

O IBM Spectrum Protect Plus é executado em um modo de avaliação por um período de tempo limitado. É necessária uma chave do produto válida para ativar recursos do IBM Spectrum Protect Plus indefinidamente.

Antes de Iniciar

Salve a chave do produto em um computador com acesso à Internet e registre o local da chave.

Procedimento

Para fazer upload da chave do produto, conclua as seguintes etapas:

1. Em um navegador suportado, insira a seguinte URL:

```
https://HOSTNAME:8090/
```

Em que *HOSTNAME* é o endereço IP da máquina virtual na qual o aplicativo é implementado.

2. Na janela de login, selecione **Tipo de autenticação > Sistema**. Insira a senha `serveradmin` para acessar o Console de Administração. A senha padrão é `sppDP758` .
É solicitado que insira uma nova senha para acessar o Console Administrativo no primeiro login.
3. Clique em **Gerenciar suas licenças** .
4. Clique em **Escolher arquivo** e, em seguida, procure a chave do produto em seu computador.
5. Clique em **Fazer Upload de Nova Licença** .
6. Clique em **Logout** .

O que Fazer Depois

Depois de fazer upload da chave do produto, conclua a seguinte ação:

Ação	Como
Inicie IBM Spectrum Protect Plus a partir de um navegador da web suportado.	Consulte “Inicie o IBM Spectrum Protect Plus” na página 71 .

Editando portas de firewall

Use os exemplos fornecidos como uma referência para abrir portas de firewall em servidores proxy VADP remotos ou servidores de aplicativos. Deve-se restringir o tráfego de porta somente para a rede ou os adaptadores necessários.

Red Hat Enterprise Linux 7 e mais recente e CentOS 7 e mais recente

abrindo portas em servidores proxy VADP remotos ou servidores de aplicativos

Use o comando a seguir para listar as portas abertas:

```
firewall-cmd --list-ports
```

Use o comando a seguir para listar zonas:

```
firewall-cmd --get-zones
```

Use o comando a seguir para listar a zona que contém a porta Ethernet `eth0`:

```
firewall-cmd --get-zone-of-interface=eth0
```

Use o comando a seguir para abrir a porta `8098` para o tráfego TCP. Este comando não é permanente.

```
firewall-cmd --add-port 8098/tcp
```

Use o comando a seguir para abrir a porta `8098` para tráfego TCP depois de reiniciar as regras de firewall.

Use este comando para fazer as mudanças persistentes:

```
firewall-cmd --permanent --add-port 8098/tcp
```

Para desfazer a mudança para a porta, use este comando:

```
firewall-cmd --remove-port 8098/tcp
```

Use o comando a seguir para abrir um intervalo de portas:

```
firewall-cmd --permanent --add-port 60000-61000/tcp
```

Use o comando a seguir para recarregar as regras de firewall com as atualizações de firewall:

```
firewall-cmd --reload
```

SUSE Linux Enterprise Server 12

Edite as opções de firewalls de segurança avançada do SUSE Linux Enterprise Server 12 no menu **Segurança e usuários**. Especifique o novo intervalo de portas requerido e aplique as mudanças.

Configurações de firewall que usam tabelas de IP

O utilitário iptables está disponível na maioria das distribuições Linux para ativar as regras de firewall e as configurações de política. Essas distribuições Linux incluem Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 7 e mais recente, CentOS 7 e mais recente e SUSE Linux Enterprise Server 12. Antes de usar esses comandos, verifique quais zonas de firewall estão ativadas por padrão. Dependendo da configuração da zona, os termos INPUT e OUTPUT podem ter que ser renomeados para corresponder a uma zona para a regra necessária.

Para o Red Hat Enterprise Linux 7 e mais recente, consulte os comandos de exemplo a seguir:

Use o comando a seguir para listar as políticas de firewall atuais:

```
sudo iptables -S sudo iptables -L
```

Use o comando a seguir para abrir a porta 8098 para tráfego TCP de entrada por meio de uma sub-rede interna <172.31.1.0/24>:

```
sudo iptables -A INPUT -p tcp -s 172.31.1.0/24 --dport 8098 -j ACCEPT
```

Use o comando a seguir para abrir a porta 8098 para o tráfego TCP de saída para a sub-rede interna <172.31.1.0/24>:

```
sudo iptables -A OUTPUT -p tcp -d 172.31.1.0/24 --sport 8098 -j ACCEPT
```

Use o comando a seguir para abrir a porta 8098 para o tráfego TCP de saída para a sub-rede interna <10.11.1.0/24> e somente para o adaptador de porta Ethernet eth1:

```
sudo iptables -A OUTPUT -o eth1 -p tcp -d 10.11.1.0/24 --sport 8098 -j ACCEPT
```

Use o comando a seguir para abrir a porta 8098 para o tráfego TCP de entrada para um intervalo de endereços IP de CES (10.11.1.5 a 10.11.1.11) e somente para o adaptador de porta Ethernet eth1:

```
sudo iptables -A INPUT -i eth1 -p tcp -m iprange --dst-range 10.11.1.5-10.11.1.11 --dport 8098 -j ACCEPT
```

Use o comando a seguir para permitir que um adaptador de porta Ethernet eth1 de rede interna se comunique com um adaptador de porta Ethernet de rede externa eth0:

```
sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT. Esse exemplo é para Red Hat Enterprise Linux 7 e mais recente, especificamente.
```

Use o comando a seguir para abrir a porta 8098 para tráfego de entrada da sub-rede 10.18.0.0/24 na porta Ethernet eth1 dentro da zona pública:

```
iptables -A IN_public_allow -i eth1 -p tcp -s 10.18.0.0/24 --dport 8098 -j ACCEPT
```

Use o comando a seguir para salvar as mudanças de regra de firewall para persistirem após um processo de reinicialização de firewall:

```
sudo iptables-save
```

Use o comando a seguir para parar e iniciar o Uncomplicated Firewall (UFW):

```
service iptables stop service iptables start
```

Capítulo 3. Instalando e configurando servidores vSnap

Cada instalação do IBM Spectrum Protect Plus requer pelo menos um servidor vSnap, que é o destino de backup primário.

Em ambientes VMware e Hyper-V, um servidor vSnap com o nome localhost é instalado automaticamente quando o dispositivo IBM Spectrum Protect Plus é implementado inicialmente. Um servidor vSnap integrado reside em uma partição do dispositivo IBM Spectrum Protect Plus e é registrado e inicializado no IBM Spectrum Protect Plus. Em ambientes de backup menores, o servidor vSnap integrado pode ser suficiente.

Em ambientes corporativos maiores, podem ser necessários servidores vSnap adicionais. Para obter orientação sobre como dimensionar, construir e posicionar servidores vSnap e outros componentes no ambiente IBM Spectrum Protect Plus, consulte o [Blueprints do IBM Spectrum Protect Plus](#).

Os servidores vSnap adicionais podem ser instalados em dispositivos virtuais ou físicos a qualquer momento após o dispositivo IBM Spectrum Protect Plus ser instalado e implementado. Após a instalação, algumas etapas de registro e de configuração são necessárias para esses servidores vSnap independentes.

O processo para a configuração de um servidor vSnap independente é o seguinte:

1. Instale o servidor vSnap.
2. Inclua o servidor vSnap como Armazenamento em disco no IBM Spectrum Protect Plus.
3. Inicialize o sistema e crie um conjunto de armazenamentos.

Instalando servidores vSnap

Ao implementar um dispositivo IBM Spectrum Protect Plus, um servidor vSnap é instalado automaticamente. Este servidor é o destino do backup primário. Em ambientes corporativos maiores, podem ser necessários servidores vSnap adicionais.

Antes de Iniciar

Execute as seguintes etapas:

1. Revise os requisitos do sistema vSnap em [“Requisitos do Componente ” na página 11](#).
2. Faça download do pacote de instalação. Diferentes arquivos de instalação são fornecidos para instalação em máquinas físicas ou virtuais. Certifique-se de fazer download dos arquivos corretos para seu ambiente. Para obter informações adicionais sobre como fazer download de arquivos, consulte [nota técnica 879861](#).

Instalando um servidor vSnap físico

Um sistema operacional Linux que suporta instalações físicas do vSnap é necessário para instalar um servidor vSnap em uma máquina física.

Procedimento

1. Instale um sistema operacional Linux que suporte instalações físicas do vSnap. Consulte [“Requisitos de instalação física do servidor vSnap” na página 16](#) para os sistemas operacionais suportados.
A configuração de instalação mínima é suficiente, mas também é possível instalar pacotes adicionais, incluindo uma interface gráfica com o usuário (GUI). A partição raiz deve ter pelo menos 8 GB de espaço livre após a instalação.
2. Edite o arquivo `/etc/selinux/config` para mudar o modo SELinux para Permissivo.

3. Execute `setenforce 0` para aplicar a configuração imediatamente sem precisar de uma reinicialização.
4. Faça download do arquivo de instalação do vSnap CC1QGML . `run` por meio do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [nota técnica 879861](#).
5. Torne o arquivo executável por meio do comando `chmod +x file_name.run` e, em seguida, execute o executável. Os pacotes do vSnap são instalados, além de todos os componentes necessários.

O que Fazer Depois

Depois de instalar o servidor vSnap, conclua a seguinte ação:

Ação	Como
Inclua o servidor vSnap no IBM Spectrum Protect Plus e configure o ambiente do vSnap.	Consulte “Gerenciando servidores vSnap” na página 56 .

Instalando um servidor vSnap virtual e um proxy VADP em um ambiente VMware

Para instalar um servidor vSnap virtual e um proxy vStorage API for Data Protection (VADP) em um ambiente VMware, implemente um modelo Open Virtualization Format (OVF). Isso cria uma máquina que contém o servidor vSnap e o proxy VADP.

Antes de Iniciar

Para facilitar a administração de rede, use um endereço IP estático para a máquina virtual. Designe o endereço usando a ferramenta NetworkManager Text User Interface (nmtui). Para obter instruções, consulte [“Designando um endereço IP estático”](#) na [página 50](#). Trabalhe com o administrador da rede ao configurar propriedades da rede.

Procedimento

1. Faça download do arquivo de instalação do modelo de servidor e de proxy CC1QEML . ova por meio do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [nota técnica 879861](#).
2. Para implementar o servidor vSnap, execute uma das seguintes ações:
 - Se estiver usando o vSphere Client para implementar o servidor vSnap, no menu **Arquivo**, clique em **Implementar modelo OVF**.
 - Se você estiver usando o vSphere Web Client, clique em **Criar/Registrar VM**, em seguida, clique em **Implementar uma máquina virtual por meio de um arquivo OVF ou OVA**. Clique em **Avançar**.
3. Especifique o local do arquivo CC1QEML . ova e selecione-o. Clique em **Avançar**.
4. Revise os detalhes do modelo e aceite o Contrato de Licença do Usuário Final. Clique em **Avançar**.
5. Forneça um nome significativo para o modelo, que se torna o nome de sua máquina virtual. Identifique um local apropriado para implementar a máquina virtual. Clique em **Avançar**.
6. Identifique o data center, servidor e conjunto de recursos para implementação. Quando solicitado que selecione o armazenamento, selecione dos armazenamentos de dados que já estão configurados no host de destino. O arquivo de configuração da máquina virtual e os arquivos de disco virtual são armazenados no armazenamento de dados. Selecione um armazenamento de dados que seja grande o suficiente para acomodar a máquina virtual e todos os seus arquivos de disco virtual. Clique em **Avançar**.
7. Selecione um formato de disco para armazenar os discos virtuais. Para otimizar o desempenho, é possível selecionar o thin provisioning, que é pré-selecionado. O thin provisioning requer menos espaço em disco, mas pode afetar o desempenho. Clique em **Avançar**.
8. Selecione redes para serem usadas pelo modelo implementado. Várias redes disponíveis no servidor ESX podem estar disponíveis ao clicar em Redes de destino. Selecione uma rede de destino que permita definir a alocação do endereço IP apropriado para a implementação da máquina virtual. Clique em **Avançar**.

9. Insira as propriedades de rede para o gateway padrão da máquina virtual, DNS, domínio de procura, endereço IP, prefixo de rede e nome do host da máquina. Se estiver usando uma configuração de Protocolo de Configuração de Host Dinâmico (DHCP), deixe todos os campos em branco.

Restrição: Um gateway padrão deve ser configurado corretamente antes da implementação do modelo OVF. Várias sequências de DNS são suportadas e devem ser separadas por vírgulas sem o uso de espaços.

O prefixo de rede deve ser especificado por um administrador da rede. O prefixo de rede deve ser inserido usando a notação CIDR; os valores válidos são 1 - 24.

10. Forneça detalhes da configuração de VADP, incluindo o endereço IP do dispositivo IBM Spectrum Protect Plus.

Para o servidor ESXi 5.5, esse prompt é mostrado quando o modelo de implementação OVF acessa a etapa **Propriedades**.

Para o servidor ESXi 6.0 e mais recente, este prompt é mostrado quando o modelo de implementação OVF acessa a etapa **Customizar modelo**.

11. Clique em **Avançar**.
12. Revise suas seleções de modelo. Clique em **Concluir** para sair do assistente e iniciar a implementação do modelo OVF. A implementação pode levar um tempo significativo.
13. Após a implementação do modelo OVF, ligue a máquina virtual recém-criada. É possível ligar a VM a partir do vSphere Client.

Importante: A VM deve permanecer ligada para que o aplicativo IBM Spectrum Protect Plus seja acessível.

14. Registre o endereço IP da VM recém-criada.

O endereço IP é necessário para acessar e registrar o servidor vSnap. Localize o endereço IP no vSphere Client, clicando na VM e revisando a guia **Resumo**.

O que Fazer Depois

Depois de instalar o servidor vSnap, conclua a seguinte ação:

Ação	Como
Inclua o servidor vSnap no IBM Spectrum Protect Plus e configure o ambiente do vSnap.	Consulte “Gerenciando servidores vSnap” na página 56.
Configure o ambiente do VADP.	Consulte “Configurando Opções para Proxies VADP” na página 110.

Instalando um servidor vSnap virtual em um ambiente Hyper-V

Para instalar um servidor vSnap em um ambiente Hyper-V, importe um modelo Hyper-V. Isso cria um dispositivo virtual que contém o servidor vSnap em uma máquina virtual Hyper-V.

Antes de Iniciar

Todos os servidores Hyper-V, incluindo nós do cluster, devem ter o serviço inicializador iSCSI Microsoft em execução em sua lista de Serviços. Configure o serviço como Automático para que ele esteja disponível quando a máquina for reiniciada.

Procedimento

1. Faça download do arquivo de instalação do vSnap CC1QFML . exe por meio do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [nota técnica 879861](#).
2. Copie o arquivo de instalação para seu servidor Hyper-V.
3. Inicie o instalador e conclua as etapas de instalação.

4. Abra o Hyper-V Manager e selecione o servidor necessário. Para requisitos do sistema Hyper-V, consulte [Requisitos do sistema para Hyper-V no Windows Server](#).
5. No menu **Ações** no Hyper-V Manager, clique em **Importar máquina virtual** e, em seguida, clique em **Avançar**. O diálogo **Localizar Pasta** é aberto.
6. Navegue para o local da pasta Máquinas virtuais dentro da pasta do vSnap descompactada. Clique em **Avançar**. O diálogo **Selecionar Máquina Virtual** é aberto.
7. Selecione vSnap e, em seguida, clique em **Avançar**. O diálogo **Escolher Tipo de Importação** é aberto.
8. Escolha o seguinte tipo de importação: **Registrar a máquina virtual no local**. Clique em **Avançar**.
9. Se o diálogo Conectar rede for aberto, especifique o comutador virtual a ser usado e, em seguida, clique em **Avançar**. O diálogo Concluir Importação é aberto.
10. Revise a descrição e, em seguida, clique em **Concluir** para concluir o processo de importação e fechar o assistente **Importar máquina virtual**. A máquina virtual é importada.
11. Clique com o botão direito na VM recém-implementada e, em seguida, clique em **Configurações**.
12. Na seção chamada IDE Controller 0, selecione **Disco rígido**.
13. Clique em **Editar** e, em seguida, clique em **Avançar**.
14. Na tela **Escolher ação**, escolha **Converter**, em seguida, clique em **Avançar**.
15. Para o Formato de Disco, selecione **VHDX**.
16. Para o Tipo de disco, selecione **Tamanho fixo**.
17. Para a opção Configurar disco, dê ao disco um novo nome e, opcionalmente, um novo local.
18. Revise a descrição e, em seguida, clique em **Concluir** para concluir a conversão.
19. Clique em **Procurar** e, em seguida, localize e selecione o VHDX recém-criado.
20. Repita as etapas 12 a 18 para cada disco na seção Controlador SCSI.
21. Ligue a VM a partir do **Hyper-V Manager**. Se solicitado, selecione a opção em que o kernel inicia no modo de resgate.
22. Use o Hyper-V Manager para identificar o endereço IP da nova máquina virtual se designado automaticamente. Para designar um IP estático à máquina virtual usando a Interface com o Usuário de Texto NetworkManager, consulte a próxima seção.
23. Se o endereço da nova VM for designado automaticamente, use o Hyper-V Manager para identificar o endereço IP. Para designar um IP estático a uma VM, use a ferramenta NetworkManager Text User Interface (nmtui). Para obter instruções, consulte [“Designando um endereço IP estático” na página 50](#).

O que Fazer Depois

Depois de instalar o servidor vSnap, conclua a seguinte ação:

Ação	Como
Inclua o servidor vSnap no IBM Spectrum Protect Plus e configure o ambiente do vSnap.	Consulte “Gerenciando servidores vSnap” na página 56 .

Gerenciando servidores vSnap

Para ativar tarefas de backup e restauração, pelo menos um dispositivo virtual IBM Spectrum Protect Plus e pelo menos um servidor vSnap são necessários. O servidor vSnap pode ser localizado no dispositivo IBM Spectrum Protect Plus ou em seu próprio dispositivo, ou pode ser uma instalação física do vSnap. Cada local do servidor vSnap deve ser incluído para ser reconhecido pelo IBM Spectrum Protect Plus.

Incluindo um servidor vSnap como um provedor de armazenamento de backup

O servidor vSnap integrado é registrado no IBM Spectrum Protect Plus quando o dispositivo é implementado. Deve-se incluir quaisquer servidores adicionais que estão instalados em dispositivos virtuais ou físicos para que eles sejam reconhecidos pelo IBM Spectrum Protect Plus.

Antes de Iniciar

Depois de incluir um servidor vSnap como um provedor de armazenamento de backup, talvez seja necessário configurar e administrar determinados aspectos do vSnap, como configuração de rede ou gerenciamento do conjunto de armazenamentos. Para obter mais informações, consulte [“Referência de administração do servidor vSnap”](#) na página 62.

Procedimento

Para incluir um servidor vSnap como um dispositivo de armazenamento de backup, conclua as seguintes etapas:

1. Efetue logon no console do servidor vSnap com o ID do usuário `serveradmin`. A senha inicial é `sppDP758`.
É solicitado que mude esta senha durante o primeiro logon.
2. Execute o comando **`vsnap user create`** para criar um nome do usuário e senha para o servidor vSnap.
3. Inicie a interface com o usuário do IBM Spectrum Protect Plus inserindo o nome do host ou endereço IP da máquina virtual na qual o IBM Spectrum Protect Plus está implementado em um navegador suportado.
4. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Disco**.
5. Clique em **Incluir armazenamento em disco**.
6. Preencha os campos na área de janela **Propriedades de armazenamento**:

Hostname/IP

Insira o endereço IP ou o nome do host resolvível do armazenamento de backup.

Site

Selecione um site para o armazenamento de backup. As opções disponíveis são **Primário**, **Secundário** ou **Incluir um novo site**. Se mais de um site primário, secundário ou definido pelo usuário estiver disponível para o IBM Spectrum Protect Plus, o site com a maior quantidade de armazenamento disponível será usado primeiro.

Nome de Usuário

Insira o nome do usuário para o servidor vSnap criado na etapa “2” na página 57.

Password

Insira a senha para o usuário.

7. Clique em **Salvar**.

O IBM Spectrum Protect Plus confirma uma conexão de rede e inclui o dispositivo de armazenamento de backup no banco de dados.

O que Fazer Depois

Depois de incluir um provedor de armazenamento de backup, execute as seguintes ações:

Ação	Como
Inicialize o servidor vSnap.	Consulte “Inicializando o servidor vSnap” na página 58.
Expandir o conjunto de armazenamentos vSnap.	Consulte “Expandindo um conjunto de armazenamentos vSnap” na página 60.
Se necessário, configure e administre determinados aspectos do vSnap, como configuração de rede ou gerenciamento do conjunto de armazenamentos.	“Referência de administração do servidor vSnap” na página 62

Tarefas relacionadas

[“Inicie o IBM Spectrum Protect Plus”](#) na página 71

Inicie o IBM Spectrum Protect Plus para começar a usar o aplicativo e seus recursos.

Editando Configurações para um Servidor vSnap

É possível editar as definições de configuração para um servidor vSnap para refletir mudanças no ambiente IBM Spectrum Protect Plus.

Procedimento

Para editar as configurações para um servidor vSnap, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Disco**.
2. Clique no ícone editar  que está associado a um servidor vSnap.
A área de janela **Editar armazenamento** é exibida.
3. Revise as configurações do servidor vSnap e, em seguida, clique em **Salvar**.

Excluindo um servidor vSnap

É possível excluir um servidor vSnap que não é mais usado em seu ambiente IBM Spectrum Protect Plus.

Procedimento

Para excluir um servidor vSnap, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Disco**.
2. Clique no ícone excluir  que está associado a um servidor vSnap.
3. Clique em **Sim** para excluir o servidor do IBM Spectrum Protect Plus.

Inicializando o servidor vSnap

O processo de inicialização prepara um novo servidor vSnap para ser utilizado, carregando e configurando componentes de software e inicializando a configuração interna. Este é um processo único que deve ser executado apenas para novas instalações.

Sobre Esta Tarefa

Como parte do processo de inicialização, o vSnap cria um conjunto de armazenamentos usando todos os discos não utilizados disponíveis no sistema. Cada uma das implementações baseadas em OVA do vSnap contém um disco virtual padrão não utilizado de 100 GB que é usado para criar o conjunto.

Se nenhum disco não utilizado for localizado, o processo de inicialização será concluído sem criar um conjunto.

Para obter informações sobre como expandir, criar e administrar conjuntos de armazenamentos, consulte [“Gerenciamento de armazenamento” na página 63](#).

É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou o console do servidor vSnap para inicializar os servidores vSnap.

Para servidores que são implementados em um ambiente virtual, a interface com o usuário fornece um método simples para executar a operação de inicialização.

Para servidores que são implementados em um ambiente físico, o console do servidor vSnap oferece mais opções para inicializar o servidor, incluindo a capacidade de criar um conjunto de armazenamentos usando opções avançadas de redundância e uma lista específica de discos.

Concluindo uma inicialização simples

Para preparar um servidor vSnap para uso, é necessário inicializar o servidor vSnap. Use o IBM Spectrum Protect Plus para inicializar um servidor vSnap que é implementado em um ambiente virtual.

Sobre Esta Tarefa

Para a instalação integrada do vSnap, que é registrada como parte de uma instalação do IBM Spectrum Protect Plus, é solicitado que inicie o processo de inicialização na primeira vez que efetuar login na interface com o usuário. Nenhuma etapa adicional é necessária.

Procedimento

Para inicializar um servidor vSnap usando a interface com o usuário do IBM Spectrum Protect Plus, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Disco**.
2. No menu **Ações** que está associado ao servidor, selecione o método de inicialização:

Inicializar com Criptografia

Ative a criptografia de dados de backup no servidor vSnap.

Inicializar

Inicialize o servidor vSnap sem a criptografia ativada.

O processo de inicialização é executado no segundo plano e não requer nenhuma interação adicional com o usuário. A conclusão do processo pode levar de 5 a 10 minutos.

Concluindo uma Inicialização Avançada

Use o console do servidor vSnap para inicializar um servidor vSnap que está implementado em um ambiente físico. A inicialização usando o console do servidor vSnap oferece mais opções para inicializar o servidor, incluindo a capacidade de criar um conjunto de armazenamentos usando as opções avançadas de redundância e uma lista específica de discos.

Procedimento

Para inicializar um servidor vSnap usando o console do servidor vSnap, conclua as seguintes etapas:

1. Efetue login no console do servidor vSnap com o ID do usuário `serveradmin`. A senha inicial é `sppDP758`.
Também é possível usar um ID do usuário que tenha privilégios de administrador do vSnap que é criado usando o comando `vsnap user create`. Para obter informações adicionais sobre como usar comandos de console, consulte [“Referência de administração do servidor vSnap”](#) na página 62.
2. Execute o comando `vsnap system init --skip_pool`. O comando não requer nenhuma interação adicional e conclui todas as tarefas de inicialização, exceto a criação de um conjunto de armazenamentos. A conclusão do processo pode levar de 5 a 10 minutos.

O que Fazer Depois

Depois de concluir a inicialização, conclua a seguinte ação:

Ação	Como
Criar um conjunto de armazenamentos	Consulte “Gerenciamento de armazenamento” na página 63.

Configurando opções de armazenamento vSnap

É possível configurar opções adicionais relacionadas ao armazenamento para um servidor vSnap.

Procedimento

Para configurar as opções para um servidor vSnap, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Disco**.

2. Clique no ícone gerenciar  que está associado ao servidor vSnap e, em seguida, expanda a seção **Opções de armazenamento**. Configure as opções de armazenamento.

Ativar Compactação

Se ativado, cada bloco de dados recebido será compactado usando um algoritmo de compactação antes de ser gravado no conjunto de armazenamentos. A compactação consome uma quantidade moderada de recursos de CPU adicionais.

Ativar Deduplicação

Se ativado, cada bloco de dados recebido será submetido a hash e comparado com blocos existentes no conjunto de armazenamentos. Se a compactação estiver ativada, os dados serão comparados depois de serem compactados. Blocos duplicados são ignorados em vez de serem gravados no conjunto. A deduplicação é desativada por padrão porque consome uma grande quantidade de recursos de memória (proporcional à quantidade de dados no conjunto) para manter a tabela de deduplicação de hashes de blocos.

Modo de Gravação Síncrona

A desativação de gravações síncronas pode levar à perda de dados e ao dano silencioso de dados de backup se o servidor de armazenamento tiver um encerramento inesperado ou reinicializar durante uma tarefa de backup. Não desative esta opção a menos que o servidor de armazenamento resida em um ambiente estável que esteja adequadamente protegido contra falhas de hardware e de energia.

Criptografia Ativada

Esta opção exibe o status de criptografia do servidor vSnap. A criptografia pode ser ativada somente durante a inicialização do vSnap. Esta opção serve apenas para propósitos informativos.

3. Clique em **Salvar**.

Expandindo um conjunto de armazenamentos vSnap

Se o IBM Spectrum Protect Plus relatar que um servidor vSnap está atingindo sua capacidade de armazenamento, o conjunto de armazenamentos do vSnap deverá ser expandido. Para expandir um conjunto de armazenamentos do vSnap, primeiro deve-se incluir discos virtuais ou físicos no servidor vSnap, incluindo discos virtuais na máquina virtual do vSnap ou incluindo discos físicos no servidor físico vSnap. Consulte a documentação do vSphere para obter informações sobre como criar discos virtuais adicionais.

Procedimento

Para expandir um conjunto de armazenamentos do vSnap, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Disco**.
2. Selecione **Ações > Varrer novamente** para o servidor vSnap que você deseja varrer novamente.
3. Clique no ícone gerenciar  que está associado ao servidor vSnap e, em seguida, expanda a seção **Incluir novos discos no armazenamento de backup**.
4. Inclua e salve os discos selecionados. O conjunto do vSnap se expande pelo tamanho dos discos que são incluídos.

Estabelecendo uma parceria de replicação para um servidor vSnap

Usando a replicação de armazenamento de backup, é possível fazer backup de dados de forma assíncrona de um servidor vSnap para outro.

Antes de Iniciar

Todos os servidores vSnap devem estar no mesmo nível de versão para que a replicação funcione. A replicação entre diferentes versões não é suportada.

Procedimento

Para estabelecer uma parceria de replicação, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Disco**.
2. Clique no ícone gerenciar  que está associado ao servidor vSnap no qual você deseja incluir uma parceria de replicação e, em seguida, expanda a seção **Configurar parceiros de armazenamento**.
3. Clique no ícone incluir .
4. Na lista **Selecionar parceiro**, selecione um servidor vSnap com o qual estabelecer uma parceria de replicação.
5. Clique em **Incluir Parceiro**.

O que Fazer Depois

Depois de criar uma parceria de replicação, conclua a seguinte ação para ativar a replicação:

Ação	Como
Selecione a opção Replicação de armazenamento de backup na política de ANS que está associada à tarefa de backup.	Consulte “Criando uma política de SLA” na página 89

Alterando a taxa de rendimento de transferência de transferência

Mude o rendimento para replicação de site e operações de transferência para que seja possível gerenciar a atividade de rede em um planejamento definido.

Procedimento

1. Na área de janela de navegação, clique em **Configuração do sistema > Site** para abrir a área de janela **Propriedades do site**.
2. Clique no ícone editar  que está associado ao site para o qual você deseja mudar o rendimento.
3. Clique em **Enable Throttle**.
A taxa do rendimento é exibida em MB/s.
4. Ajuste o rendimento:
 - Mude a taxa de rendimento com as setas para cima e para baixo.
 - Altere o valor de dados. As opções incluem Bytes/s, KB/s, MB/s ou GB/s.

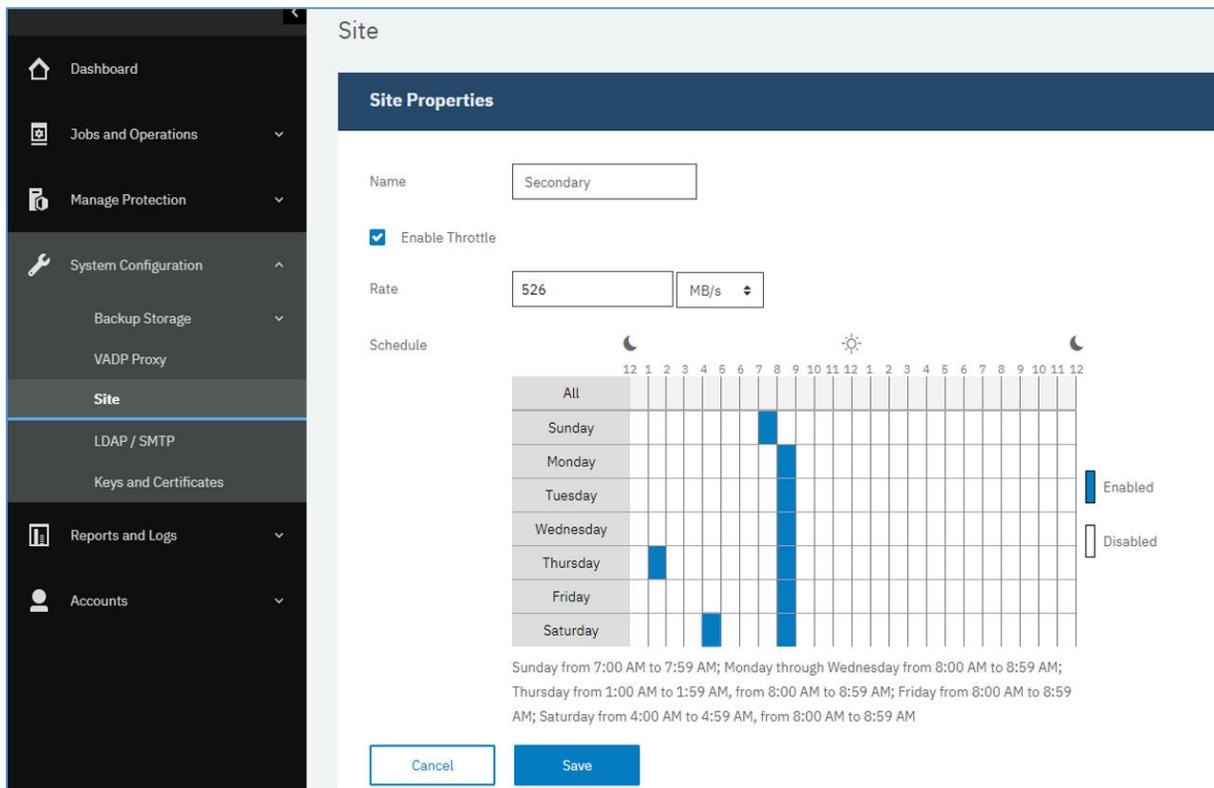


Figura 4. Ativando diferentes reguladores para diferentes horários para melhorar o rendimento

5. Selecione horários para o rendimento mudado na tabela de planejamento semanal, ou especifique um dia e hora para a taxa mudada.

Nota: Para limpar um intervalo de tempo, clique nele. As seleções planejadas são listadas abaixo da tabela de planejamento.

6. Clique em **Salvar** para confirmar as mudanças e fechar o painel.

Referência de administração do servidor vSnap

Após o servidor vSnap ter sido instalado, registrado e inicializado, o IBM Spectrum Protect Plus gerencia automaticamente seu uso como um destino de backup. Volumes e capturas instantâneas são criados e gerenciados automaticamente com base nas políticas de ANS que são definidas no IBM Spectrum Protect Plus.

No entanto, ainda pode ser necessário configurar e administrar alguns aspectos do vSnap, como configuração de rede ou gerenciamento do conjunto de armazenamentos.

Gerenciando o vSnap usando a interface da linha de comandos

A interface da linha de comandos do vSnap é o principal meio de administrar o vSnap. Execute o comando **vsnap** para acessar a interface da linha de comandos. O comando pode ser chamado pelo ID do usuário `serveradmin` ou por qualquer outro usuário do sistema operacional que tenha privilégios de administrador do vSnap. Use o comando **vsnap user create** para criar usuários adicionais do sistema operacional que têm esses privilégios. A senha inicial do `serveradmin` é `sppDP758`.

Por padrão, não são designados privilégios `sudo` ao usuário `serveradmin`. Para designar privilégios `sudo` ao usuário `serveradmin`, efetue login na interface da linha de comandos do servidor vSnap e insira o seguinte comando:

```
echo "serveradmin ALL = (ALL) NOPASSWD: ALL" > /etc/sudoers.d/serveradmin
```

A interface da linha de comandos consiste em vários comandos e subcomandos que gerenciam vários aspectos do sistema. Consulte [“Gerenciamento de armazenamento”](#) na página 63 e [“Gerenciamento de rede”](#) na página 66 para obter detalhes sobre como usar esses comandos. Também é possível transmitir a sinalização **--help** para qualquer comando ou subcomando para visualizar a ajuda de uso, por exemplo, **vsnap --help** ou **vsnap pool create --help**.

Gerenciando o vSnap usando a interface com o usuário do IBM Spectrum Protect Plus

Algumas das operações mais comuns também podem ser concluídas a partir da interface com o usuário do IBM Spectrum Protect Plus. Efetue login na interface com o usuário e clique em **Configuração do sistema > Armazenamento de backup > Disco** na área de janela de navegação. Clique no ícone gerenciar  para um servidor vSnap para gerenciá-lo.

Tarefas relacionadas

[“Instalando servidores vSnap”](#) na página 53

Ao implementar um dispositivo IBM Spectrum Protect Plus, um servidor vSnap é instalado automaticamente. Este servidor é o destino do backup primário. Em ambientes corporativos maiores, podem ser necessários servidores vSnap adicionais.

[“Gerenciando servidores vSnap”](#) na página 56

Para ativar tarefas de backup e restauração, pelo menos um dispositivo virtual IBM Spectrum Protect Plus e pelo menos um servidor vSnap são necessários. O servidor vSnap pode ser localizado no dispositivo IBM Spectrum Protect Plus ou em seu próprio dispositivo, ou pode ser uma instalação física do vSnap. Cada local do servidor vSnap deve ser incluído para ser reconhecido pelo IBM Spectrum Protect Plus.

Gerenciamento de armazenamento

É possível configurar e administrar conjuntos de armazenamentos para um servidor vSnap.

Gerenciando discos

O vSnap cria um conjunto de armazenamentos usando discos fornecidos para o servidor vSnap. No caso de implementações virtuais, os discos podem ser RDM ou discos virtuais fornecidos a partir de armazenamentos de dados em qualquer armazenamento auxiliar. No caso de implementações físicas, os discos podem ser armazenamento local ou SAN conectado ao servidor físico. Os discos locais podem já ter redundância externa ativada por meio de um controlador RAID de hardware, mas se não tiverem, o vSnap também pode criar conjuntos de armazenamentos baseados em RAID para redundância interna.

Os discos que estão conectados aos servidores vSnap devem ser thick provisioned. Se os discos forem thin provisioned, o servidor vSnap não terá uma visualização precisa do espaço livre no conjunto de armazenamentos, o que poderá levar a distorção de dados, se o armazenamento de dados subjacente ficar sem espaço.

Se o vSnap foi implementado como parte de um dispositivo virtual, ele já contém um disco virtual iniciador de 100 GB que pode ser usado para criar um conjunto. É possível incluir mais discos antes ou depois de criar um conjunto e usá-los de forma apropriada para criar um conjunto maior ou expandir um conjunto existente. Se os logs de tarefas relatarem que um servidor vSnap está atingindo sua capacidade de armazenamento, discos adicionais podem ser incluídos no conjunto do vSnap. Como alternativa, a criação de novas políticas de ANS forçará os backups a usarem um vSnap alternativo.

É essencial proteger-se contra dano causado por um armazenamento de dados do VMware em um servidor vSnap que atinge sua capacidade. Crie um ambiente estável para servidores vSnap virtuais que não usam configurações do RAID utilizando VMDKs thick provisioned. A replicação para servidores vSnap externos fornece proteção adicional.

Um servidor vSnap será invalidado se o conjunto do vSnap for excluído ou se um disco do vSnap for excluído em uma configuração do RAID não redundante. Todos os dados no servidor vSnap serão perdidos. Se o seu servidor vSnap se tornar invalidado, você deve cancelar o registro dele usando a interface do IBM Spectrum Protect Plus e, em seguida, executar a tarefa de manutenção. Após a conclusão, o servidor vSnap pode ser registrado novamente.

Gerenciando a criptografia

Para ativar a criptografia de dados de backup em um servidor vSnap, selecione **Inicializar com a criptografia ativada** quando inicializar o servidor. As configurações de criptografia não podem ser mudadas após a inicialização do servidor e a criação de um conjunto. Todos os discos de um conjunto do vSnap usam o mesmo arquivo de chave de criptografia, que é gerado na criação do conjunto. Os dados são criptografados quando estão inativos no servidor vSnap.

A criptografia vSnap utiliza o algoritmo a seguir:

Nome da cifra

Advanced Encryption Standard (AES)

Modo Cipher

xts-plain64

Tecla

256 bits

Hashing de cabeçalho do Linux Unified Key Setup (LUKS)

sha256

Gerenciando chaves de criptografia

Os arquivos de chave de criptografia de disco gerados na criação do conjunto são armazenados no diretório `/etc/vsnap/keys/` em cada servidor vSnap. Para propósitos de recuperação de desastre, faça backup dos arquivos-chave manualmente fora do servidor vSnap. Após a criação de um conjunto, use os seguintes comandos como o usuário `serveradmin` para copiá-lo para um local temporário e, em seguida, copie-o para um local de backup desejado, seguro, fora do host vSnap.

```
mkdir /tmp/keybackup-$(hostname)
```

```
sudo cp -r /etc/vsnap/keys /tmp/keybackup-$(hostname)
```

Detectando discos

Se você incluir discos em um servidor vSnap, use a linha de comandos ou a interface com o usuário do IBM Spectrum Protect Plus para detectar os discos recém-conectados.

Linha de comandos: Execute o comando **`vsnap disk rescan`**.

Interface com o usuário: Clique em **Configuração do sistema > Armazenamento de backup > Disco** na área de janela de navegação e, em seguida, clique no menu **Ações**, próximo ao servidor vSnap relevante e selecione **Varrer novamente**.

Mostrando discos

Execute o comando **`vsnap disk show`** para listar todos os discos que estão no sistema vSnap.

A coluna `USED AS` na saída mostra se cada disco está em uso. Qualquer disco que estiver não formatado e não particionado é marcado como não utilizado; caso contrário, eles são marcados como utilizados pela tabela de partição ou pelo sistema de arquivos que é descoberto neles.

Somente os discos que estão marcados como não utilizados são elegíveis para criação ou inclusão em um conjunto de armazenamentos. Se um disco que você planeja incluir em um conjunto de armazenamentos não for visto como não utilizado pelo vSnap, isso pode ocorrer porque ele estava em uso anteriormente e, portanto, contém remanescentes de uma tabela de partição ou sistema de arquivos mais antigo. É possível corrigir isso usando comandos do sistema, como **`parted`** ou **`dd`** para limpar a tabela de partição de disco.

Mostrando informações do conjunto de armazenamentos

Execute o comando **vsnap pool show** para visualizar informações sobre cada conjunto de armazenamentos.

Criando um conjunto de armazenamentos

Se você concluiu o procedimento de inicialização simples descrito em “Concluindo uma inicialização simples” na página 58, um conjunto de armazenamentos foi criado automaticamente e as informações nesta seção não são aplicáveis.

Para concluir uma inicialização avançada, use o comando **vsnap pool create** para criar um conjunto de armazenamentos manualmente. Antes de executar o comando, certifique-se de que um ou mais discos não utilizados estejam disponíveis, conforme descrito em “Mostrando discos” na página 64. Para obter informações sobre as opções disponíveis, transmita a sinalização **--help** para qualquer comando ou subcomando.

Especifique um nome de exibição fácil e simples para o conjunto e uma lista de um ou mais discos. Se nenhum disco for especificado, todos os discos não utilizados disponíveis serão usados. É possível optar por ativar a compactação e a deduplicação para o conjunto durante a criação. Também é possível atualizar as configurações de compactação/deduplicação posteriormente usando o comando **vsnap pool update**.

O tipo de conjunto especificado durante a criação do conjunto de armazenamento determina a redundância do conjunto:

raid0

Esta é a opção padrão quando nenhum tipo de conjunto é especificado. Nesse caso, o vSnap considera que seus discos tenham redundância externa, por exemplo, se você usar discos virtuais em um armazenamento de dados suportado por armazenamento redundante. Nesse caso, o conjunto de armazenamentos não terá redundância interna.

Depois que um disco tiver sido incluído em um conjunto raid0, ele não pode ser removido. Desconectar o disco resultará na indisponibilidade do conjunto, o que pode ser resolvido apenas destruindo e recriando o conjunto.

raid5

Ao selecionar esta opção, o conjunto é composto de um ou mais grupos RAID5, cada um consistindo em três ou mais discos. O número de grupos RAID5 e o número de discos em cada grupo dependem do número total de discos especificados durante a criação do conjunto. Com base no número de discos disponíveis, o vSnap escolhe valores que aumentam a capacidade total enquanto também asseguram a redundância ideal de metadados vitais.

raid6

Ao selecionar esta opção, o conjunto é composto de um ou mais grupos RAID6, cada um consistindo em quatro ou mais discos. O número de grupos RAID6 e o número de discos em cada grupo dependem do número total de discos especificados durante a criação do conjunto. Com base no número de discos disponíveis, o vSnap escolhe valores que aumentam a capacidade total enquanto também asseguram a redundância ideal de metadados vitais.

Expandindo um conjunto de armazenamentos

Antes de expandir um conjunto, certifique-se de que um ou mais discos não utilizados estejam disponíveis, conforme descrito em “Mostrando discos” na página 64.

Use a linha de comandos ou a interface com o usuário do IBM Spectrum Protect Plus para expandir um conjunto de armazenamentos.

Linha de comandos: Execute o comando **vsnap pool expand**. Para obter informações sobre as opções disponíveis, transmita a sinalização **--help** para qualquer comando ou subcomando.

Interface com o usuário: Clique em **Configuração do sistema > Armazenamento de backup > Disco** na área de janela de navegação. Clique no ícone gerenciar  para um servidor vSnap para gerenciá-lo e, em

seguida, expanda a guia **Incluir novos discos**. A guia exibe todos os discos não utilizados descobertos no sistema. Selecione um ou mais discos e clique em **Salvar** para incluí-los no conjunto de armazenamentos.

Gerenciamento de rede

Configure e administre serviços de rede para um servidor vSnap.

Mostrando informações da interface de rede

Execute o comando **vsnap network show** para listar interfaces de rede e os serviços que estão associados a cada interface.

Por padrão, os seguintes serviços de vSnap estão disponíveis para todas as interfaces de rede:

mgmt

Este serviço é usado para tráfego de gerenciamento entre o IBM Spectrum Protect Plus e o vSnap.

nfs

Este serviço é usado para tráfego de dados ao fazer backup de dados usando NFS.

iscsi

Este serviço é usado para tráfego de dados ao fazer backup de dados usando iSCSI.

smb

Este serviço é usado para tráfego de dados ao fazer backup de dados usando SMB/CIFS.

repl

Este serviço é usado para tráfego de dados entre servidores vSnap durante a replicação.

Modificando Serviços Associados às Interfaces de Rede

Execute o comando **vsnap network update** para modificar serviços que estão associados a uma interface. Por exemplo, se estiver usando uma interface dedicada para tráfego de dados para melhorar o desempenho.

As seguintes opções são exigidas:

--id <id>

Insira o ID da interface a ser atualizado.

-- serviços < services>

Especifique **all** ou uma lista separada por vírgula de serviços a serem ativados na interface. A seguir estão os valores válidos: **mgmt**, **nfs**, **smb** e **iscsi**.

Se um serviço estiver disponível em mais de uma interface, o IBM Spectrum Protect Plus poderá usar qualquer uma das interfaces.

Certifique-se de que o serviço **mgmt** permaneça ativado na interface que foi usada para registrar o servidor vSnap no IBM Spectrum Protect Plus.

Desinstalando um servidor vSnap

É possível remover um servidor vSnap de seu ambiente IBM Spectrum Protect Plus.

Antes de Iniciar

Certifique-se de que nenhuma tarefa use políticas de ANS que definem o servidor vSnap como um local de backup. Para visualizar as políticas de ANS que estão associadas a tarefas, consulte a página **Backup** para o hypervisor ou aplicativo que está planejado para backup. Por exemplo, para tarefas de backup do VMware, clique em **Gerenciar proteção > Hypervisors > VMware**.

Procedimento

1. Efetue logon no console do servidor vSnap com o ID do usuário **serveradmin**. A senha inicial é **sppDP758**.

Também é possível usar um ID do usuário que tenha privilégios de administrador do vSnap criados usando o comando **vsnap user create**. Para obter informações adicionais sobre como usar comandos de console, consulte [“Referência de administração do servidor vSnap”](#) na página 62.

2. Execute os seguintes comandos:

```
systemctl stop vsnap  
yum remove vsnap
```

3. Opcional: Se você não planeja reinstalar o servidor vSnap após ele ser desinstalado, remova os dados e a configuração executando os comandos a seguir:

```
rm -rf /etc/vsnap  
rm -rf /etc/nginx  
rm -rf /etc/uwsgi.d  
rm -f /etc/uwsgi.ini
```

4. Reinicialize o sistema para assegurar que os módulos kernel estejam descarregados e remova os discos de dados que contêm dados do conjunto vSnap.

Nota: Para desinstalar o IBM Spectrum Protect Plus em um ambiente do Hyper-V, exclua o dispositivo SPP do Hyper-V e, em seguida, exclua o diretório de instalação.

Resultados

Depois que um servidor vSnap é desinstalado, a configuração é retida no diretório `/etc/vsnap`. A configuração será reutilizada se o servidor vSnap for reinstalado. A configuração será removida se você executou os comandos opcionais para remover os dados de configuração.

Capítulo 4. Desiniciando para um Início Rápido

Para começar a usar o IBM Spectrum Protect Plus, deve-se concluir as etapas que incluem a definição de recursos que você deseja proteger e a criação de políticas de acordo de nível de serviço (SLA), também conhecidas como políticas de backup, para esses recursos. Esta seção de introdução fornece as etapas básicas para configurar e começar a usar o IBM Spectrum Protect Plus para fazer backup de dados. Outras tarefas, como transferência e restauração de dados, são discutidas em detalhes em outras áreas da documentação.

Antes de iniciar, assegure-se de que você seguiu as instruções no [Blueprints do IBM Spectrum Protect Plus](#) para determinar como dimensionar, construir e colocar os componentes em seu ambiente do IBM Spectrum Protect Plus e de que as tarefas listadas no [“Roteiro de implementação do produto”](#) na [página 11](#) estão concluídas.

Conforme mostrado na tabela a seguir, as tarefas de instalação e configuração iniciais são concluídas pelo *administrador de infraestrutura* do IBM Spectrum Protect Plus. Por padrão, a conta do usuário `admin` é criada para uso pelo administrador de infraestrutura para iniciar o aplicativo pela primeira vez.

Portanto, as tarefas de backup e restauração do hypervisor e do aplicativo de banco de dados são concluídas pelo *administrador do aplicativo*. No entanto, um único administrador pode ser responsável por todas as tarefas em seu ambiente.

Ação	Owner	
Iniciar o IBM Spectrum Protect Plus	Administrador de infraestrutura e administrador de aplicativo	<p>O administrador de infraestrutura inicia o aplicativo pela primeira vez usando a conta do usuário <code>admin</code> padrão com a senha <code>password</code>. O administrador é solicitado a reconfigurar o nome de usuário dessa conta depois de efetuar login. O administrador não pode reconfigurar o nome de usuário como <code>admin</code>, <code>root</code> ou <code>test</code>.</p> <p>Após a primeira inicialização, o administrador do aplicativo pode iniciar o aplicativo usando essa conta do usuário ou outra conta criada pelo administrador de infraestrutura.</p>

Ação	Owner	
“Gerenciar sites” na página 72	Administrador de infraestrutura	<p>Um site é usado para agrupar servidores vSnap com base em um local físico ou lógico para ajudar a identificar e interagir rapidamente com os dados de backup. Um site é designado a um servidor vSnap quando o servidor é incluído no IBM Spectrum Protect Plus.</p> <p>Os sites padrão são nomeados Primário e Secundário, mas um site customizado também pode ser criado e designado quando o servidor vSnap é incluído.</p> <p>Antes de continuar com as ações a seguir, revise os sites disponíveis e determine se você deseja incluir novos sites ou modificar os existentes.</p>
Criar políticas de backup	Administrador de infraestrutura	<p>As políticas de backup definem os parâmetros que são aplicados a tarefas de backup. Esses parâmetros incluem a frequência e a retenção de backups e as opções para replicar dados de um servidor vSnap para outro e para transferir dados de backup para o armazenamento de backup secundário para proteção de longo prazo.</p> <p>As políticas de backup também definem o site de destino para fazer backup de dados. Um site pode conter um ou mais servidores vSnap.</p> <p>As políticas de backup são chamadas de políticas de SLA no IBM Spectrum Protect Plus.</p>
Criar uma conta do usuário para o administrador do aplicativo	Administrador de infraestrutura	As contas do usuário determinam os recursos e funções que estão disponíveis para o usuário.
Incluir recursos para proteger	Administrador de aplicativos	Recursos são servidores para hypervisors ou aplicativos de banco de dados que hospedam dados que você deseja proteger.

Ação	Owner	
<u>Incluir recursos em uma definição de tarefa</u>	Administrador de aplicativos	As definições de tarefa associam os recursos que você deseja proteger com uma ou mais políticas de SLA. As opções e planejamentos que estão definidos nas políticas de ANS são usados para tarefas de backup para os recursos.
<u>Inicie a tarefa de backup</u>	Administrador de aplicativos	As tarefas de backup são iniciadas conforme definido na política de ANS que está associada à definição de tarefa. Também é possível iniciar manualmente uma tarefa.
<u>Executar um relatório</u>	Administrador de aplicativos	O IBM Spectrum Protect Plus fornece vários relatórios predefinidos que podem ser executados com parâmetros padrão ou modificados para criar relatórios customizados.

Inicie o IBM Spectrum Protect Plus

Inicie o IBM Spectrum Protect Plus para começar a usar o aplicativo e seus recursos.

Procedimento

Para iniciar o IBM Spectrum Protect Plus, conclua as etapas a seguir:

1. Em um navegador da web suportado, insira a seguinte URL:

```
https:// host_name
```

Em que *host_name* é o endereço IP da máquina virtual na qual o aplicativo está implementado. Isso conecta você ao IBM Spectrum Protect Plus.

2. Digite o nome de usuário e a senha para efetuar login.

Caso esta seja sua primeira vez efetuando login, o nome de usuário padrão será `admin` e a senha será `password`. Você será solicitado a reconfigurar o nome de usuário e a senha padrão. Não é possível reconfigurar o nome de usuário como `admin`, `root` ou `test`.

3. Clique em **Efetuar Sign In**.

4. Se estiver efetuando login no IBM Spectrum Protect Plus pela primeira vez, é solicitado que conclua as seguintes ações:

- Altere a senha `serveradmin`. A senha inicial é `sppDP758`. O usuário `serveradmin` é usado para acessar o console administrativo e o dispositivo virtual IBM Spectrum Protect Plus. A senha para `serveradmin` deve ser mudada antes de acessar o console administrativo e o dispositivo virtual IBM Spectrum Protect Plus.
- Inicie o processo de inicialização para o servidor vSnap integrado. Selecione **Inicializar** ou **Inicializar com a criptografia ativada** para criptografar dados no servidor.

Gerenciar sites

Um site é usado para agrupar servidores vSnap com base em um local físico ou lógico para ajudar a identificar e interagir rapidamente com os dados de backup. Um site é designado a um servidor vSnap quando o servidor é incluído no IBM Spectrum Protect Plus.

Sobre Esta Tarefa

Um site é designado a um servidor vSnap quando o servidor é incluído no IBM Spectrum Protect Plus. Revise os sites disponíveis clicando em **Configuração do sistema > Site** na área de janela de navegação e decida se você deseja incluir novos sites ou editar os existentes para seus servidores vSnap.

Nota: É possível mudar o nome do site e outras opções para os sites Primário e Secundário padrão.

O site Demo está disponível somente para o servidor vSnap integrado. Não é possível usar esse site com qualquer outro servidor vSnap.

Procedimento

Para incluir ou editar um site, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Configuração do sistema > Site**.
2. Para incluir novos sites ou editar sites existentes, tome a ação apropriada:

Ação	Como
Inclua um novo site.	<ol style="list-style-type: none">a. Clique em Incluir Site.b. Insira um nome de site.c. Opcional: selecione Ativar regulador para gerenciar o rendimento para operações de replicação e transferência de site, conforme descrito em “Incluindo um Site” na página 271.d. Clique em Salvar.
Edite um site.	<ol style="list-style-type: none">a. Clique em Editar site.b. Clique no ícone editar  que está associado a um site.c. Opcional: selecione Ativar regulador para gerenciar o rendimento para operações de replicação e transferência de site, conforme descrito em “Editando um Site” na página 272.d. Clique em Salvar.

Conceitos relacionados

[“Componentes do Produto” na página 1](#)

A solução do IBM Spectrum Protect Plus é fornecida como um dispositivo virtual autocontido que inclui componentes de armazenamento e de movimentação de dados.

[“Gerenciando sites” na página 271](#)

Um *site* é uma construção de política do IBM Spectrum Protect Plus que é usada para gerenciar o posicionamento de dados em um ambiente.

Criar políticas de backup

As políticas de backup, que também são referidas como políticas de acordo de nível de serviço (ANS), definem parâmetros que são aplicados a tarefas de backup. Estes parâmetros incluem a frequência e a retenção de backups.

Sobre Esta Tarefa

As três políticas de ANS padrão são Ouro, Prata e Bronze. É possível usar essas políticas como elas são ou modificá-las. Também é possível criar políticas de ANS customizadas.

Se uma máquina virtual estiver associada a várias políticas de ANS, certifique-se de que as políticas não sejam planejadas para execução simultaneamente. Planeje as políticas de ANS para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de ANS.

Para fins de exemplo, esta tarefa não inclui instruções para ativar a replicação para servidores vSnap ou para transferência ou arquivamento para o armazenamento de backup secundário, que são recursos opcionais. Para obter informações sobre como configurar esses recursos na política de ANS, consulte [“Criando uma política de SLA” na página 89](#).

As cópias de backup de dados são chamadas de capturas instantâneas.

Procedimento

Para criar uma política de ANS, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Visão geral de política**.
2. Clique em **Incluir política de SLA**.
A área de janela **Nova política de ANS** é exibida.
3. No campo **Nome**, insira um nome que forneça uma descrição significativa da política de ANS.
4. Na seção **Proteção operacional**, em **Política principal**, configure as seguintes opções para operações de backup. Essas operações ocorrem nos servidores vSnap que estão definidos na janela **Configuração do sistema > Armazenamento de backup > Disco**.

Retenção

Especifique o período de retenção para as capturas instantâneas de backup.

Desativar Programação

Selecione esta caixa de seleção para criar a política principal sem definir uma frequência ou horário de início. As políticas criadas sem um planejamento podem ser executadas on-demand.

Frequência

Insira a frequência para operações de backup.

Start Time

Insira a data e hora em que deseja que a operação de backup seja iniciada.

Site de Destino

Selecione o site de backup de destino para fazer backup de dados.

Um site pode conter um ou mais servidores vSnap. Se mais de um servidor vSnap estiver em um site, o servidor IBM Spectrum Protect Plus gerenciará o posicionamento de dados nos servidores vSnap.

Somente sites que estão associados a um servidor vSnap são mostrados nessa lista. Os sites que são incluídos no IBM Spectrum Protect Plus, mas não estão associados a um servidor vSnap, não são mostrados.

Utilizar apenas armazenamento em disco criptografado

Selecione esta caixa de seleção para fazer backup de dados para servidores vSnap criptografados, se seu ambiente incluir uma mistura de servidores criptografados e não criptografados.

Restrição: Se esta opção estiver selecionada e nenhum servidor vSnap criptografado estiver disponível, a tarefa associada falhará.

O exemplo a seguir mostra uma nova política de ANS chamada Copper que é executada a cada 3 dias à meia-noite com uma retenção de 1 mês:

The screenshot displays the 'New SLA Policy' configuration window in IBM Spectrum Protect Plus. The sidebar on the left contains navigation links: Dashboard, Jobs and Operations, Manage Protection, Policy Overview (selected), File Restore, Hypervisors, Applications, IBM Spectrum Protect Plus, System Configuration, Reports and Logs, and Accounts. The main content area is titled 'Policy Overview' and 'New SLA Policy'. The 'Name' field is 'Copper'. The 'Operational Protection' section includes 'Main Policy' with 'Retention' set to 1 Months and 'Frequency' set to 3 Days. The 'Start Time' is 01/29/2019 00:00. The 'Target Site' is Primary. The 'Replication Policy' section has 'Backup Storage Replication' checked, 'Frequency' set to 1 Days, 'Start Time' set to 01/29/2019 01:00, and 'Target Site' set to Secondary. A checkbox 'Same retention as source selection' is checked. 'Cancel' and 'Save' buttons are at the bottom.

Figura 5. Criando uma política de SLA

5. Clique em **Salvar**. A política de ANS agora pode ser aplicada a definições de tarefa de backup, conforme mostrado em [“Incluir recursos em uma definição de tarefa”](#) na página 78.

Conceitos relacionados

[“Replicar dados de armazenamento de backup”](#) na página 5

Ao ativar a replicação de dados de backup, os dados de um servidor vSnap são replicados de forma assíncrona para outro servidor vSnap. Por exemplo, é possível replicar dados de backup de um servidor vSnap em um site primário para um servidor vSnap em um site secundário.

[“Transfload para armazenamento de backup secundário”](#) na página 6

O servidor vSnap é o local de backup primário para capturas instantâneas. Todos os ambientes do IBM Spectrum Protect Plus têm pelo menos um servidor vSnap. Opcionalmente, é possível transferir capturas instantâneas de um servidor vSnap para o armazenamento de backup secundário.

[“Gerenciar políticas SLA para operações de backup”](#) na página 89

As políticas de Acordo de nível de serviço (ANS), também conhecidas como políticas de backup, definem parâmetros para tarefas de backup. Esses parâmetros incluem a frequência e o período de retenção de backups e a opção para replicar ou transferir dados de backup. É possível usar políticas de ANS predefinidas ou customizá-las para atender às suas necessidades.

Criar uma conta do usuário para o administrador do aplicativo

Crie uma conta do usuário para um administrador que possa executar operações de backup e restauração para os hypervisors ou aplicativos que estão em seu ambiente.

Antes de Iniciar

Para propósitos de exemplo, as seguintes etapas mostram como criar uma conta para um usuário individual que é responsável por proteger dados do VMware. Essa conta usa uma função de usuário e um grupo de recursos existentes.

Para criar uma conta para um grupo LDAP, consulte [“Criando uma conta do usuário para um grupo LDAP”](#) na página 306.

Para criar funções de usuário customizado e grupos de recursos, consulte [“Criando um Grupo de Recursos”](#) na página 297 e [“Criando uma função”](#) na página 302

Procedimento

Para criar uma conta para um administrador do aplicativo, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Usuário**.
2. Clique em **Incluir Usuário**. A área de janela **Incluir Usuário** é exibida.
3. Clique em **Selecione o tipo de usuário ou grupo que você deseja incluir > Novo usuário individual**.
4. Insira um nome e uma senha para o administrador do aplicativo.
5. Na seção **Designar função**, selecione **Administrador de VM**.
As permissões são mostradas na seção **Grupos de permissão**.

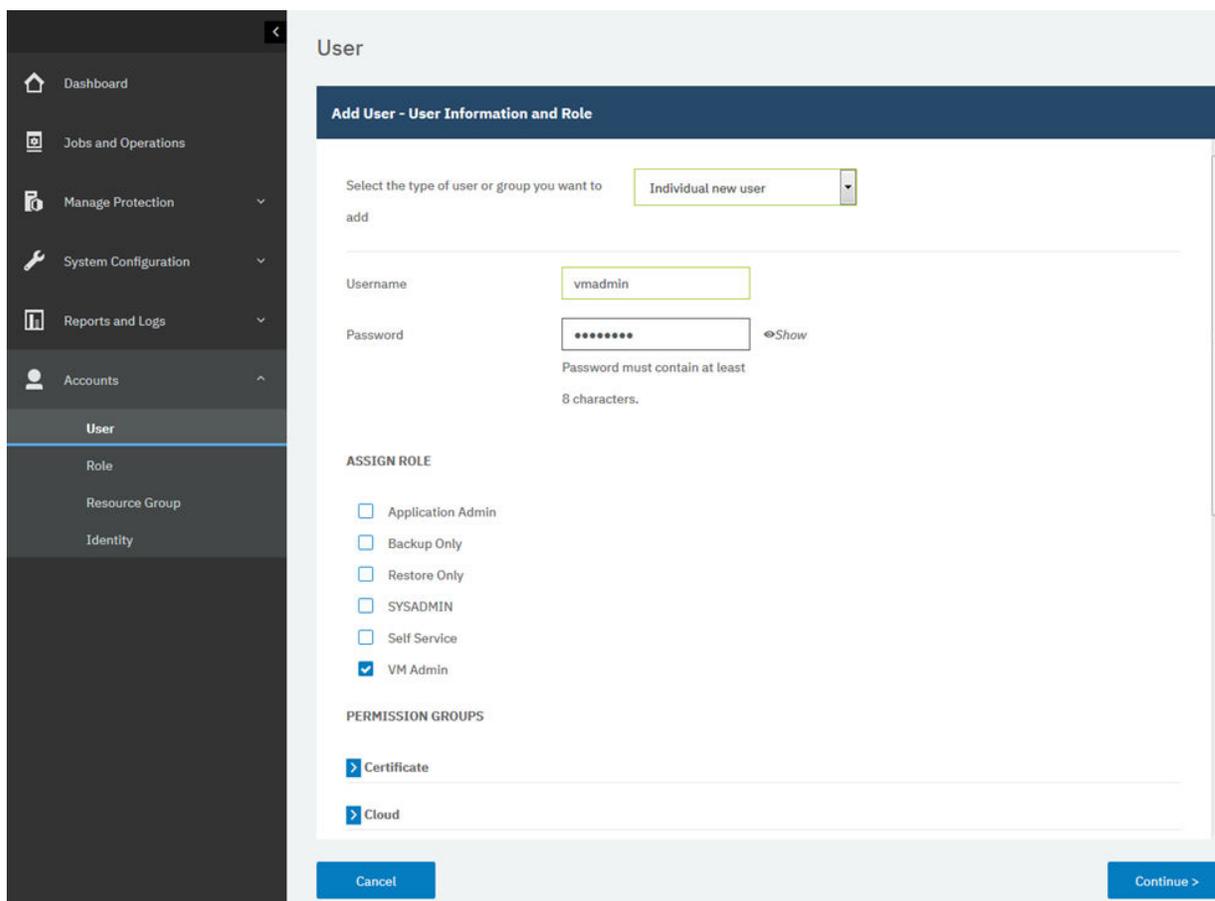


Figura 6. Criando uma conta do usuário e designando uma função

6. Clique em **Continuar**.
7. Na seção **Incluir usuários - Designar recursos**, selecione o grupo de recursos **Todos os recursos** e, em seguida, clique em **Incluir recursos**.
O grupo de recursos é incluído na seção **Recursos selecionados**.

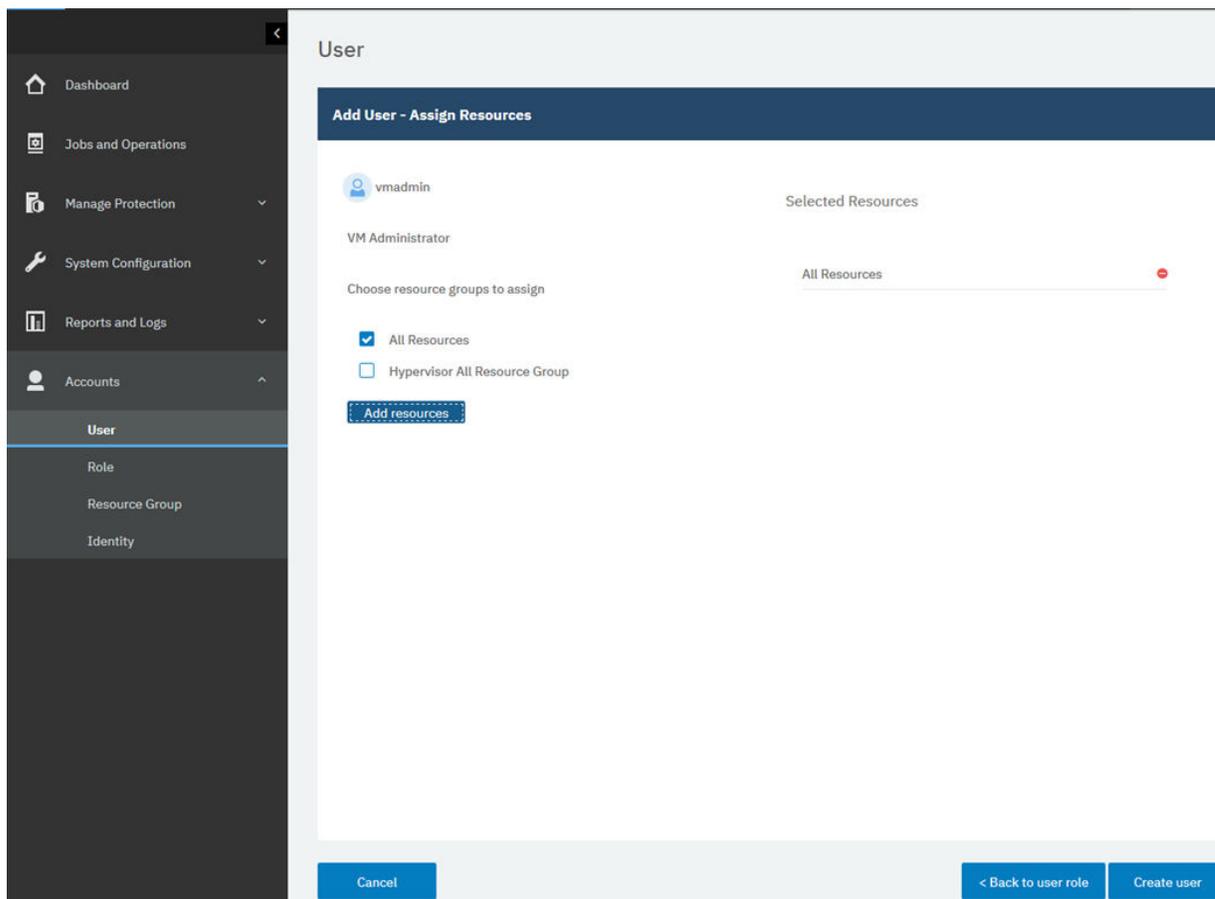


Figura 7. Selecionando um grupo de recursos para a conta do usuário

8. Clique em **Criar usuário** .

Conceitos relacionados

“Gerenciando o acesso de” na página 297

Usando o controle de acesso baseado na função, é possível configurar os recursos e permissões disponíveis para contas do usuário do IBM Spectrum Protect Plus.

Incluir recursos para proteger

Recursos são servidores para hypervisors ou aplicativos que hospedam dados que você deseja proteger. Depois que um recurso é registrado, um inventário do recurso é capturado e incluído no inventário do IBM Spectrum Protect Plus, permitindo concluir tarefas de backup e restauração, bem como executar relatórios.

Sobre Esta Tarefa

Por exemplo, esta tarefa descreve como incluir um recurso do VMware. Para incluir outros recursos, consulte as instruções por tipo de recurso em [Capítulo 7, “Protegendo hypervisors”](#), na página 95 e [Capítulo 8, “Protegendo Aplicativos”](#), na página 137.

Procedimento

Para incluir uma instância do vCenter Server, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Clique em **Gerenciar vCenter** e, em seguida, clique em **Incluir vCenter**.
3. Preencha os campos na seção **Propriedades do vCenter**:

Hostname/IP

Insira o endereço IP resolvível ou um caminho e nome de máquina resolvíveis.

Usar usuário existente

Ative para selecionar um nome do usuário e senha inseridos anteriormente para a instância do vCenter Server.

Nome de Usuário

Insira seu nome de usuário para a instância do vCenter Server.

Password

Insira sua senha para a instância do vCenter Server.

Porta

Insira a porta de comunicações da instância do vCenter Server. Selecione a caixa de seleção **Usar SSL** para ativar uma conexão Secure Sockets Layer (SSL) criptografada. A porta padrão típica é 80 para conexões não SSL ou 443 para conexões SSL.

4. Na seção **Opções**, configure a seguinte opção:

Número máximo de VMs a serem processadas simultaneamente por servidor ESX e por ANS

Configure o número máximo de capturas instantâneas da VM simultâneas a serem processadas no servidor ESX.

O exemplo a seguir mostra campos preenchidos.

The screenshot displays the VMware Backup configuration page for vCenter. On the left is a navigation sidebar with options like Dashboard, Jobs and Operations, Manage Protection, VMware, System Configuration, Reports and Logs, and Accounts. The main content area is titled 'VMware' and 'Manage vCenter'. It contains the following fields:

- Hostname/IP: 192.0.2.0
- Use existing user:
- Username: admin_192.0.2.0
- Password: masked with dots
- Port: 443
- Use SSL:
- Options: Maximum number of VM's to process concurrently per ESX server: 3

Buttons for 'Cancel' and 'Save' are at the bottom, along with a 'Create Restore Job' button in the top right.

Figura 8. Incluindo uma Instância do vCenter Server

5. Clique em **Salvar**.

O IBM Spectrum Protect Plus confirma uma conexão de rede, inclui o recurso no banco de dados e, em seguida, cataloga o recurso. Se aparecer uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se suas entradas estiverem corretas e a conexão for malsucedida, entre em contato com um administrador de rede para verificar e, possivelmente, corrigir as conexões.

Incluir recursos em uma definição de tarefa

Antes de poder fazer backup de um recurso, você deve criar uma definição de tarefa que associe o recurso a uma ou mais políticas de backup, também referidas como políticas de ANS.

Sobre Esta Tarefa

Para propósitos de exemplo, esta tarefa descreve como selecionar uma política de ANS para recursos que estão em um VMware vCenter. Para selecionar uma política para outros recursos, consulte as instruções por tipo de recurso em [Capítulo 7, “Protegendo hypervisors”](#), na página 95 e [Capítulo 8, “Protegendo Aplicativos”](#), na página 137.

Procedimento

Para selecionar uma política de ANS, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Selecione os recursos dos quais você deseja fazer backup. É possível selecionar todos os recursos em um vCenter ou realizar drill down para selecionar recursos específicos.

Use a função de procura para procurar recursos disponíveis e alternar os recursos exibidos usando o filtro **Visualizar**. As opções disponíveis são **MVs e modelos, MVs, Armazenamento de dados, Tags e categoriase Hosts e clusters**. As tags, que são aplicadas no vSphere, permitem designar metadados a máquinas virtuais.

O exemplo a seguir mostra um disco rígido específico que é selecionado para backup:

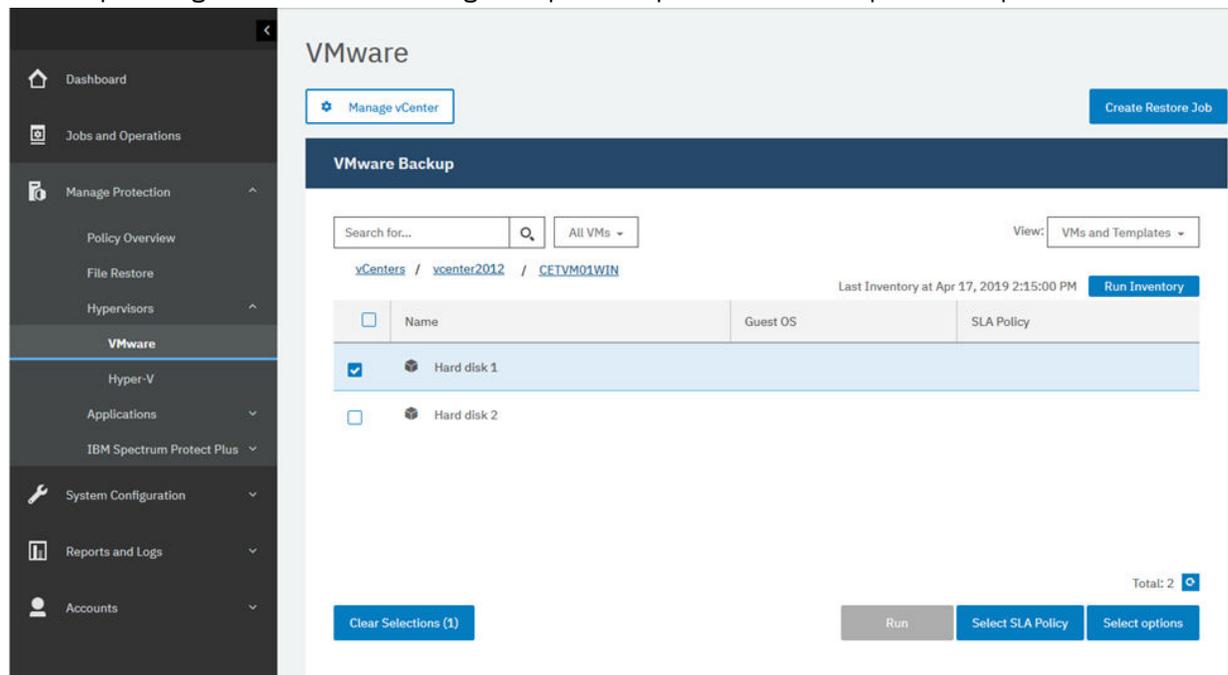


Figura 9. Selecionando recursos para backup

3. Clique em **Selecionar política de ANS** para incluir uma ou mais políticas de ANS que atendem aos critérios de dados de backup para a definição de tarefa.

O exemplo a seguir mostra a política de ANS **Copper** selecionada:

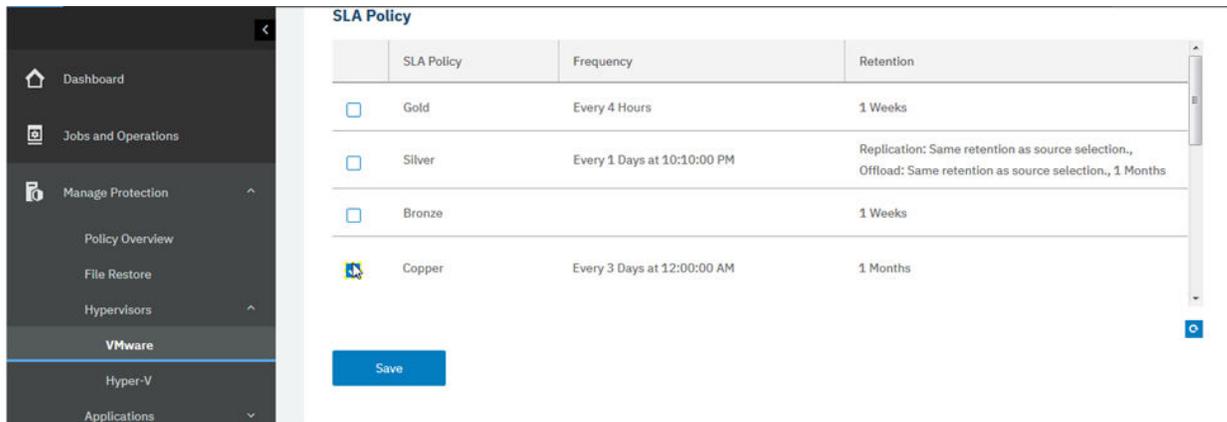


Figura 10. Selecionando uma política de SLA

4. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.
5. Opcional: Para configurar opções adicionais, clique em **Selecionar opções** e siga as instruções em [“Fazendo backup dos dados de VMware”](#) na página 103.
6. Clique em **Salvar**.

Depois que a definição de tarefa é salva, os discos de máquina virtual (VMDKs) disponíveis em uma máquina virtual são descobertos e mostrados quando a opção **VMs e modelos** é selecionada no filtro **Visualização**. Por padrão, esses VMDKs são designados à mesma política de ANS que a máquina virtual. Opcionalmente, para definir uma política mais granular ao excluir VMDKs individuais, siga as instruções em [“Excluindo VMDKs da política de ANS para uma tarefa”](#) na página 107.

Resultados

A tarefa é executada conforme definido pelas políticas de ANS selecionadas, ou é possível executar a tarefa manualmente clicando em **Tarefas e operações** e, em seguida, clicando na guia **Lista de políticas e de tarefas**. Para obter instruções, consulte [“Inicie a tarefa de backup”](#) na página 79.

Conceitos relacionados

[“Protegendo IBM Spectrum Protect Plus”](#) na página 247

Proteja o aplicativo IBM Spectrum Protect Plus fazendo backup dos bancos de dados subjacentes para cenários de recuperação de desastre. Definições de configuração, recursos registrados, pontos de restauração, configurações de armazenamento de backup, dados de procura e informações de tarefa são submetidos a backup para um servidor vSnap definido na política de ANS associada.

Inicie a tarefa de backup

É possível iniciar uma tarefa de backup on demand fora do planejamento que é configurado pela política de SLA.

Procedimento

Para iniciar uma tarefa de backup on demand, conclua as seguintes etapas:

1. Na navegação, clique em **Tarefas e operações**, e abra a guia **Planejamento** .
Caso a tarefa não seja uma tarefa planejada, mas uma tarefa on demand, clique na guia **Histórico da tarefa** .
2. Escolha a tarefa que você deseja executar e clique em **Ações > Iniciar**, conforme mostrado no exemplo a seguir:

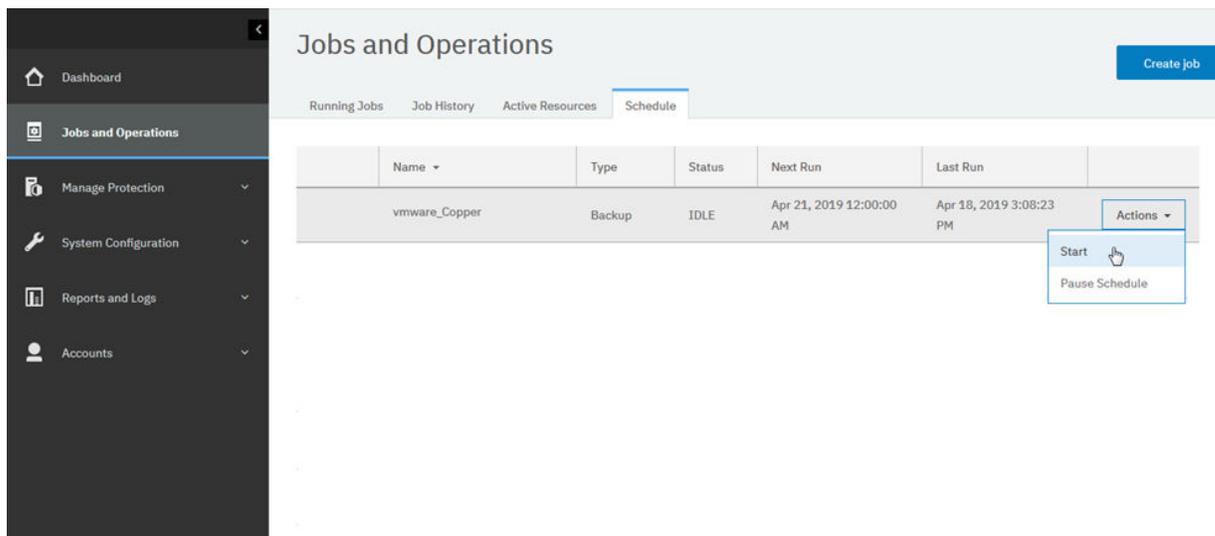


Figura 11. Iniciando uma Tarefa

3. Para visualizar o log da tarefa em detalhes, clique na tarefa na guia **Tarefas em execução**.

A tela de log mostra os detalhes a seguir:

- Status: mostra se a mensagem é um erro, um aviso ou uma mensagem de informação.
 - Horário: mostra o registro de data e hora da mensagem.
 - ID: mostra o identificador exclusivo para a mensagem, se aplicável.
 - Descrição: mostra do que se trata a mensagem.
4. É possível fazer download de um log da tarefa da página clicando em **Fazer download do .zip**. Se você deseja cancelar a tarefa, clique em **Ações > Cancelar**.
 5. Clique no menu **Ações** que está associado à tarefa que você deseja iniciar e clique em **Iniciar**, conforme mostrado no exemplo a seguir:

Conceitos relacionados

“Tarefas e operações” na página 251

Use a janela **Tarefas e operações** para monitorar tarefas, revisar o histórico da tarefa, planejar tarefas, visualizar recursos ativos e executar novamente ou pausar tarefas e planejamentos.

Executar um relatório

Execute relatórios com parâmetros padrão predefinidos ou parâmetros customizados.

Procedimento

Para executar um relatório, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Expanda um tipo de relatório e selecione um relatório para ser executado, conforme mostrado no exemplo a seguir:

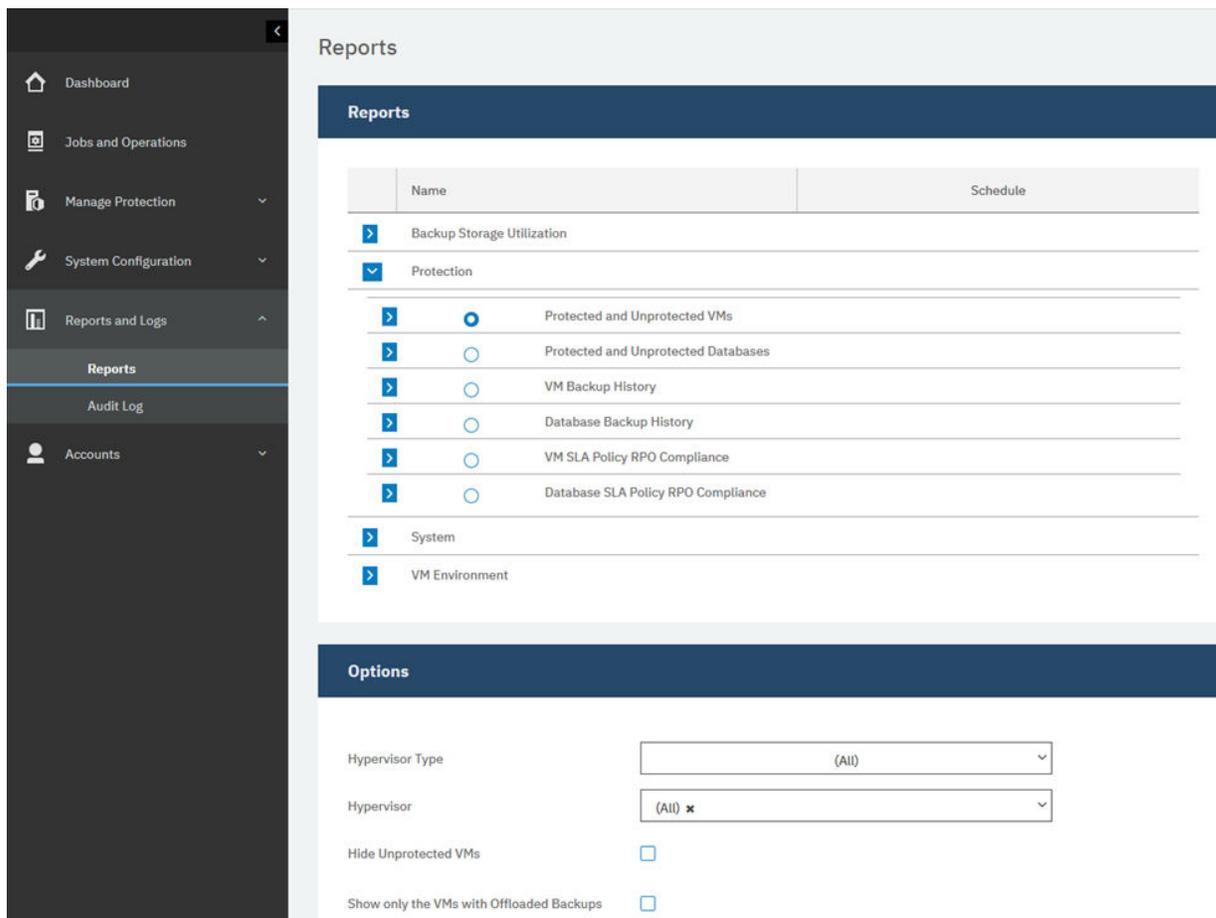


Figura 12. Selecionando um relatório para execução

3. Execute o relatório com parâmetros customizados ou parâmetros padrão:

- Para executar o relatório com parâmetros customizados, configure os parâmetros na seção **Opções** e clique em **Executar**. Os parâmetros são exclusivos para cada relatório.
- Para executar o relatório com parâmetros padrão, clique em **Executar**.

Conceitos relacionados

“Gerenciando relatórios e logs” na página 289

O IBM Spectrum Protect Plus fornece vários relatórios predefinidos que podem ser customizados para atender aos requisitos de relatório. Também é fornecido um log de ações que os usuários concluem no IBM Spectrum Protect Plus.

Capítulo 5. Atualizando componentes do IBM Spectrum Protect Plus

É possível atualizar o dispositivo virtual IBM Spectrum Protect Plus, servidores vSnap e os servidores proxy VADP para obter os recursos e aprimoramentos mais recentes. As correções e atualizações de software são instaladas usando o console administrativo do IBM Spectrum Protect Plus ou a interface da linha de comandos para esses componentes.

Para obter informações sobre arquivos de atualização disponíveis e como obtê-los de um site de download da IBM, consulte [nota técnica 879861](#).

Antes de atualizar componentes do IBM Spectrum Protect Plus, revise os requisitos de hardware e de software para os componentes para confirmar quaisquer mudanças que possam ter ocorrido de versões anteriores.

Revise as seguintes restrições e dicas:

- Deve-se atualizar separadamente os servidores vSnap que não estão em dispositivos virtuais IBM Spectrum Protect Plus.
- O processo de atualização por meio do console administrativo atualiza os recursos do IBM Spectrum Protect Plus e os componentes de infraestrutura subjacentes, incluindo o sistema operacional e o sistema de arquivos. Não use outro método para atualizar esses componentes.
- Não atualize nenhum dos componentes subjacentes para o IBM Spectrum Protect Plus, a menos que o componente seja fornecido em um pacote de atualização do IBM Spectrum Protect Plus. As atualizações de infraestrutura são gerenciadas por recursos de atualização da IBM. O console administrativo é o principal meio para atualizar os recursos do IBM Spectrum Protect Plus e os componentes de infraestrutura subjacentes, incluindo o sistema operacional e o sistema de arquivos.

Execute as seguintes ações:

- Antes de atualizar seus componentes, é importante fazer backup do ambiente IBM Spectrum Protect Plus, conforme descrito em [“Fazendo backup do aplicativo IBM Spectrum Protect Plus”](#) na página 247.
- Após a atualização do IBM Spectrum Protect Plus, ele não pode retroceder para uma versão anterior sem uma captura instantânea de máquina virtual. Crie uma captura instantânea de máquina virtual de seu ambiente antes de atualizar o IBM Spectrum Protect Plus. Posteriormente, se você desejar retroceder o IBM Spectrum Protect Plus para uma versão anterior, deverá ter uma captura instantânea de máquina virtual. Quando o upgrade for concluído com sucesso, remova a captura instantânea de máquina virtual.

Atualizando o dispositivo virtual IBM Spectrum Protect Plus

Use o console administrativo do IBM Spectrum Protect Plus para atualizar o dispositivo virtual. A atualização do IBM Spectrum Protect Plus poderá ser executada off-line ou on-line se você tiver acesso externo à Internet.

Antes de Iniciar

É possível atualizar o IBM Spectrum Protect Plus V10.1.2 ou mais recente diretamente para a versão atual. Se você estiver usando a V10.1.1, será necessário atualizar para a V10.1.2 e, em seguida, atualizar para a versão atual. Para obter instruções sobre como atualizar da V10.1.1 para a V10.1.2, consulte [Atualizando o dispositivo virtual IBM Spectrum Protect Plus para a versão 10.1.2](#).

Antes de iniciar o processo de atualização, conclua as seguintes etapas:

1. Assegure-se de que o ambiente do IBM Spectrum Protect Plus seja submetido a backup antes de executar atualizações. Para obter mais informações sobre como fazer backup de seu ambiente, consulte [“Fazendo backup do aplicativo IBM Spectrum Protect Plus”](#) na página 247.

2. Para atualizações off-line, faça download da atualização de pré-requisito do IBM Spectrum Protect Plus denominada CC1QHML . iso para um diretório no computador que está executando o navegador para o console administrativo. O arquivo de atualização é instalado primeiro.
3. Certifique-se de que nenhuma tarefa esteja em execução durante o procedimento de atualização. Pause o planejamento para quaisquer tarefas que tenham um status de INATIVO ou CONCLUÍDO.

Para obter uma lista de imagens de download, incluindo a atualização do sistema operacional necessária para o dispositivo virtual, consulte [nota técnica 879861](#).

Sobre Esta Tarefa

Quando você tem acesso à Internet, é possível escolher executar o procedimento de atualização on-line. Se você não tiver acesso à Internet, será possível executar o procedimento de atualização off-line.

Procedimento

Para atualizar o dispositivo virtual IBM Spectrum Protect Plus, conclua as seguintes etapas:

1. Em um navegador da web suportado, acesse o console administrativo inserindo o endereço a seguir:

```
https:// hostname : 8090 /
```

em que *hostname* é o endereço IP da máquina virtual em que o aplicativo é implementado.

2. Na janela de login, selecione um dos seguintes tipos de autenticação na lista **Tipo de autenticação**:

Tipo de Autenticação	Informações de login
IBM Spectrum Protect Plus	Para efetuar login como um usuário do IBM Spectrum Protect Plus com privilégios SYSADMIN, insira seu nome de usuário e senha de administrador. Se você efetuar login usando a conta do usuário admin, será solicitado que reconfigure o nome do usuário e a senha. Não é possível reconfigurar o nome de usuário como admin, root ou test.
Sistema (recomendado)	Para efetuar login como um usuário do sistema, insira a senha do administrador do servidor. A senha padrão é sppDP758. É solicitado que mude esta senha durante o primeiro login.

3. Clique em **Atualizações e gerenciamento de hotfix** para abrir a página de gerenciamento de atualizações.

Se você tiver acesso ao site FTP, public.dhe.ibm.com, o console do administrador verificará as atualizações disponíveis automaticamente e as listará.

4. Clique em **Executar atualização** para instalar as atualizações disponíveis.
 - Quando as atualizações forem instaladas com êxito, acesse a Etapa 6.
 - Se você estiver planejando instalar uma atualização por meio de um arquivo ISO, clique em **Clique aqui** para executar as atualizações off-line. Vá para a Etapa 5.

Nota: Se você desejar executar atualizações on-line, mas puder ver somente o modo off-line, verifique sua conectividade de Internet e tente acessar o site FTP, public.dhe.ibm.com.

5. Escolha a atualização que você deseja executar, conforme a seguir:

- Modo on-line: as atualizações são listadas automaticamente no repositório quando elas são disponibilizadas. Clique em **Executar atualização**.
- Modo off-line: clique em **Escolher arquivo** para procurar o arquivo transferido por download. O arquivo tem uma extensão iso ou rpm como este exemplo, <filename> . iso. Clique em **Fazer upload da imagem de atualização (ou) hotfix**.

Nota: É possível selecionar somente um arquivo de atualização por vez.

Quando a atualização estiver concluída, a máquina virtual na qual o aplicativo está implementado será reinicializada automaticamente.

Importante: Após a conclusão da atualização do IBM Spectrum Protect Plus, deve-se atualizar quaisquer servidores proxy vSnap e VADP externos em seu ambiente.

6. Limpe o cache do navegador.

O conteúdo HTML de versões anteriores do IBM Spectrum Protect Plus pode ser armazenado no cache.

7. Inicie a versão atualizada do IBM Spectrum Protect Plus.

8. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.

Localize as tarefas que você pausou.

9. No menu **Ações** para as tarefas pausadas, selecione **Planejamento de liberação**.

Tarefas relacionadas

[“Atualizando servidores vSnap” na página 85](#)

O servidor vSnap padrão é atualizado com o dispositivo IBM Spectrum Protect Plus. Deve-se atualizar servidores vSnap adicionais que estão instalados em dispositivos virtuais ou físicos separadamente.

Atualizando servidores vSnap

O servidor vSnap padrão é atualizado com o dispositivo IBM Spectrum Protect Plus. Deve-se atualizar servidores vSnap adicionais que estão instalados em dispositivos virtuais ou físicos separadamente.

Antes de Iniciar

É possível atualizar seus servidores vSnap diretamente da versão 10.1.2 ou mais recente para a versão atual. Se você estiver usando a versão 10.1.1, deverá atualizar para a versão 10.1.2 e, em seguida, atualizar para a versão atual. Para obter instruções sobre como atualizar para a versão 10.1.2, consulte [Atualizando servidores vSnap para a versão 10.1.2](#).

As tarefas de teste de restauração precisam ser concluídas antes de iniciar uma atualização para o vSnap. As tarefas que não forem concluídas ou canceladas quando um upgrade for iniciado não estarão visíveis quando a atualização for concluída. Se as tarefas não estiverem visíveis quando a atualização for concluída, execute novamente as tarefas de teste de restauração.

Também pode ser necessário atualizar o sistema operacional para os servidores vSnap antes de atualizar os servidores. Para requisitos do sistema operacional, consulte [“Requisitos do Componente” na página 11](#).

Para verificar a versão atual e o sistema operacional para os servidores vSnap, conclua as seguintes etapas:

1. Efetue logon no servidor vSnap como o usuário `serveradmin`. Se estiver usando o IBM Spectrum Protect Plus 10.1.1, efetue login usando a conta raiz.
2. Para verificar a versão do servidor vSnap e o sistema operacional, use a interface da linha de comandos do vSnap para emitir o seguinte comando:

```
informações do sistema vsnap
```

Certifique-se de que nenhuma tarefa que usa o servidor vSnap esteja em execução durante o procedimento de atualização. Pause o planejamento para quaisquer tarefas que tenham um status de INATIVO ou CONCLUÍDO.

Atualizando o sistema operacional para um servidor vSnap físico

Se você instalou o servidor vSnap em uma máquina que está executando o Red Hat Enterprise Linux, deve-se atualizar o sistema operacional para a versão 7.5 ou 7.6 antes de atualizar o servidor vSnap. Para

obter instruções sobre como atualizar o sistema operacional, consulte a documentação do Red Hat Enterprise Linux.

Tarefas relacionadas

[“Atualizando um servidor vSnap” na página 86](#)

O servidor vSnap padrão é atualizado com o dispositivo IBM Spectrum Protect Plus. Deve-se atualizar servidores vSnap adicionais que estão instalados em dispositivos virtuais ou físicos separadamente.

Atualizando o sistema operacional para um servidor vSnap virtual

Se o sistema operacional for CentOS Linux versão 7.4 ou anterior, você deve atualizar o sistema operacional antes de atualizar o servidor vSnap. Para atualizar o sistema operacional, siga as instruções em [Atualizando servidores vSnap para a versão 10.1.2](#). A instalação do versão 10.1.2 inclui o CentOS Linux versão 7.5.

Tarefas relacionadas

[“Atualizando um servidor vSnap” na página 86](#)

O servidor vSnap padrão é atualizado com o dispositivo IBM Spectrum Protect Plus. Deve-se atualizar servidores vSnap adicionais que estão instalados em dispositivos virtuais ou físicos separadamente.

Atualizando um servidor vSnap

O servidor vSnap padrão é atualizado com o dispositivo IBM Spectrum Protect Plus. Deve-se atualizar servidores vSnap adicionais que estão instalados em dispositivos virtuais ou físicos separadamente.

Antes de Iniciar

Antes de iniciar o processo de atualização, conclua as seguintes etapas:

1. Certifique-se de que tenha feito backup de seu ambiente do IBM Spectrum Protect Plus, conforme descrito em [“Fazendo backup do aplicativo IBM Spectrum Protect Plus” na página 247](#).
2. Se você estiver atualizando a partir do IBM Spectrum Protect Plus 10.1.1, deverá atualizar para a versão 10.1.2 e, em seguida, atualizar para a versão atual. Para obter instruções sobre como atualizar para a versão 10.1.2, consulte [Atualizando servidores vSnap para a versão 10.1.2](#).
3. Faça download do arquivo de atualização do vSnap CC1QGML.run e copie-o para um local provisório no servidor vSnap. Para obter informações sobre como fazer download de arquivos, consulte [nota técnica 879861](#).

Procedimento

Para atualizar um servidor vSnap, conclua as seguintes etapas:

1. Efetue logon no servidor vSnap como o usuário **serveradmin**.
2. No diretório no qual o arquivo CC1QGML.run está localizado, torne o arquivo executável e execute o instalador emitindo os comandos a seguir:

```
chmod +x CC1QGML.run
```

```
sudo ./CC1QGML.run
```

Os pacotes vSnap são instalados.

3. Inicie a versão atualizada do IBM Spectrum Protect Plus.
4. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.
Localize as tarefas que você pausou.
5. No menu **Ações** para as tarefas pausadas, selecione **Planejamento de liberação**.

Atualizando proxies VADP

A atualização do dispositivo virtual IBM Spectrum Protect Plus atualiza automaticamente todos os proxies VADP que estão associados ao dispositivo virtual. Em cenários raros, como perda de conectividade de rede, é necessário atualizar o proxy VADP manualmente.

Antes de Iniciar

Antes de iniciar, certifique-se de que tenha feito backup de seu ambiente IBM Spectrum Protect Plus, conforme descrito em [“Fazendo backup do aplicativo IBM Spectrum Protect Plus”](#) na página 247.

Procedimento

Se uma atualização de proxy VADP estiver disponível para proxies externos durante uma reinicialização do dispositivo virtual IBM Spectrum Protect Plus, a atualização será aplicada automaticamente a qualquer proxy VADP associado a uma identidade. Para associar um proxy VADP com uma identidade, navegue para **Configuração do sistema > Proxy VADP**. Clique no ícone de opções **☰** e selecione **Configurar opções**. Por meio da configuração do Usuário, selecione um nome de usuário e senha inseridos anteriormente para o servidor proxy VADP.

Para atualizar um proxy VADP manualmente, conclua as seguintes etapas:

1. Navegue para a página **Configuração do sistema > Proxy VADP** no IBM Spectrum Protect Plus.
2. A página **Proxy VADP** exibe cada servidor proxy. Se uma versão mais recente do software do proxy VADP estiver disponível, um ícone atualizar  será exibido no campo **Status**.
3. Certifique-se de que não haja tarefas ativas que usam o proxy e, em seguida, clique no ícone atualizar .

O servidor proxy entra em um estado suspenso e instala a atualização mais recente. Quando a atualização é concluída, o servidor proxy VADP continua automaticamente e entra em um estado ativado.

Se você estiver tentando atualizar como um usuário não raiz, instruções especiais precisarão ser seguidas para enviar por push-install ou push-update um proxy VADP.

1. Crie um arquivo no diretório `/etc/sudoers.d/`.

```
sudo cd /etc/sudoers.d/
```

2. Grave o texto no arquivo e salve-o pressionando CTRL+D no teclado quando concluído.

```
sudo cat > 99-vadpuser
Defaults !requiretty
vadpuser ALL=NOPASSWD: /tmp/cdm_guestapps_vadpuser/runcommand.sh
<<Press CTRL+D>>
```

3. Configure as permissões apropriadas no arquivo.

```
sudo chmod 0440 99-vadpuser
```

O que Fazer Depois

Depois de atualizar os proxies VADP, conclua a seguinte ação:

Ação	Como
Execute a tarefa de backup do VMware.	<p data-bbox="857 195 1459 258">Consulte “Fazendo backup dos dados de VMware” na página 103.</p> <p data-bbox="857 275 1451 338">Os proxies são indicados no log da tarefa por uma mensagem de log semelhante ao seguinte texto:</p> <p data-bbox="857 354 1321 464">Executar vmdkbackup remoto de MicroService: http://<proxy nodename, IP:proxy_IP_address</p>

Tarefas relacionadas

“Criando proxies do VADP” na página 108

É possível criar proxies VADP para executar tarefas de backup do VMware com o IBM Spectrum Protect Plus em ambientes Linux.

Referências relacionadas

“Editando portas de firewall” na página 51

Use os exemplos fornecidos como uma referência para abrir portas de firewall em servidores proxy VADP remotos ou servidores de aplicativos. Deve-se restringir o tráfego de porta somente para a rede ou os adaptadores necessários.

Aplicando atualizações de disponibilidade antecipada

As atualizações de disponibilidade antecipada fornecem correções para authorized program analysis reports (APARs) e problemas menores entre liberações do IBM Spectrum Protect Plus. Essas atualizações estão disponíveis em pacotes configuráveis a partir do website Fix Central Online.

Sobre Esta Tarefa

As atualizações de disponibilidade antecipada podem não conter correções para todos os componentes do IBM Spectrum Protect Plus.

Para obter instruções sobre como obter e instalar correções temporárias, consulte as informações de download que são publicadas quando as correções estão disponíveis.

Capítulo 6. Gerenciar políticas SLA para operações de backup

As políticas de Acordo de nível de serviço (ANS), também conhecidas como políticas de backup, definem parâmetros para tarefas de backup. Esses parâmetros incluem a frequência e o período de retenção de backups e a opção para replicar ou transferir dados de backup. É possível usar políticas de ANS predefinidas ou customizá-las para atender às suas necessidades.

As seguintes políticas de ANS padrão estão disponíveis. Cada política especifica uma frequência e um período de retenção para o backup. É possível usar essas políticas como elas são ou modificá-las. Também é possível criar políticas de ANS customizadas.

Ouro

Essa política é executada a cada 4 horas com um período de retenção de 1 semana.

Prata

Esta política é executada diariamente com um período de retenção de 1 mês.

Bronze

Esta política é executada diariamente com um período de retenção de 1 semana.

Para visualizar e gerenciar as políticas de backup e monitorar as máquinas virtuais e os bancos de dados que são protegidos por políticas, clique em **Gerenciar proteção > Visão geral de política** na área de janela de navegação.

Se você editar uma política de ANS existente mudando a origem de transferência em nuvem, o tipo de destino de transferência ou opções do servidor de transferência de destino, as tarefas associadas iniciarão um backup de base completo, não um backup incremental, durante a próxima execução da tarefa.

Para instalações do IBM Spectrum Protect PlusV10.1.4, uma configuração de demo do SLA está disponível para teste. Esse recurso de demonstração inclui os elementos a seguir:

- Um site de demonstração denominado **Demo**
- Uma política de SLA denominada **Demo**
- Uma configuração do vSnap local para o SLA de demonstração.

É possível optar por usar o site de demonstração para testar operações de backup e restauração. Os dados são salvos em backup na configuração local do vSnap ao executar a política SLA de demonstração.

Nota: O vSnap integrado está configurado de forma a poder ser usado somente pelo site de demonstração. Não use o vSnap integrado do IBM Spectrum Protect Plus com qualquer outro site.

Criando uma política de SLA

É possível criar políticas de ANS customizadas para definir políticas de frequência de backup, de retenção, de replicação e de transferência que são específicas de seu ambiente.

Sobre Esta Tarefa

Se uma máquina virtual estiver associada a várias políticas de ANS, certifique-se de que as políticas criadas não estejam planejadas para execução simultaneamente. Planeje as políticas de ANS para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de ANS.

Se uma tarefa de replicação de captura instantânea for iniciada antes da conclusão de um backup inicial para um servidor vSnap, os erros no log da tarefa indicam que não existem pontos de recuperação para o banco de dados. Após a conclusão do backup inicial para o servidor vSnap, execute a tarefa de replicação novamente para replicar as capturas instantâneas, conforme configurado na política de ANS.

Procedimento

Para criar uma política de ANS, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Visão geral de política**.
2. Clique em **Incluir política de SLA**.
A área de janela **Nova política de ANS** é exibida.
3. No campo **Nome**, insira um nome que forneça uma descrição significativa da política de ANS.
4. Na seção **Proteção operacional**, em **Política principal**, configure as seguintes opções para operações de backup. Essas operações ocorrem nos servidores vSnap que estão definidos na janela **Configuração do sistema > Armazenamento de backup > Disco**.

Retenção

Especifique o período de retenção para as capturas instantâneas de backup.

Desativar Programação

Selecione esta caixa de seleção para criar a política principal sem definir uma frequência ou horário de início. As políticas criadas sem um planejamento podem ser executadas on-demand.

Frequência

Insira uma frequência para operações de backup.

Start Time

Insira a data e hora em que deseja que a operação de backup seja iniciada.

Site de Destino

Selecione o site de backup de destino para fazer backup de dados.

Um site pode conter um ou mais servidores vSnap. Se mais de um servidor vSnap estiver em um site, o servidor IBM Spectrum Protect Plus gerenciará o posicionamento de dados nos servidores vSnap.

Somente sites que estão associados a um servidor vSnap são mostrados nessa lista. Os sites que são incluídos no IBM Spectrum Protect Plus, mas não estão associados a um servidor vSnap, não são mostrados.

Utilizar apenas armazenamento em disco criptografado

Selecione esta caixa de seleção para fazer backup de dados para servidores vSnap criptografados, se seu ambiente incluir uma mistura de servidores criptografados e não criptografados.

Restrição: Se esta opção estiver selecionada e não houver nenhum servidor vSnap criptografado disponível, a tarefa associada falhará.

5. Em **Política de replicação**, configure as seguintes opções para ativar a replicação assíncrona de um servidor vSnap para outro. Por exemplo, é possível replicar dados do site de backup primário para o secundário.

Requisito de Parcer: Essas opções se aplicam a parcerias de replicação estabelecidas. Para incluir uma parceria de replicação, consulte as instruções em [“Estabelecendo uma parceria de replicação para um servidor vSnap”](#) na página 60.

Replicação de armazenamento de backup

Selecione esta opção para ativar a replicação.

Desativar Programação

Selecione essa caixa de seleção para criar o relacionamento de replicação sem definir uma frequência ou horário de início.

Frequência

Insira uma frequência para operações de replicação.

Start Time

Insira a data e hora em que você deseja que a operação de replicação seja iniciada.

Site de Destino

Selecione o site de backup de destino para replicar dados.

Um site pode conter um ou mais servidores vSnap. Se mais de um servidor vSnap estiver em um site, o servidor IBM Spectrum Protect Plus gerenciará o posicionamento de dados nos servidores vSnap.

Somente sites que estão associados a um servidor vSnap são mostrados nessa lista. Os sites que são incluídos no IBM Spectrum Protect Plus, mas não estão associados a um servidor vSnap, não são mostrados.

Utilizar apenas armazenamento em disco criptografado

Selecione esta opção para replicar dados para servidores vSnap criptografados, se seu ambiente incluir uma mistura de servidores criptografados e não criptografados.

Restrição: Se esta opção estiver selecionada e não houver nenhum servidor vSnap criptografado disponível, a tarefa associada falhará.

Mesma retenção que a seleção de origem

Selecione esta opção para usar a mesma política de retenção que o servidor vSnap de origem. Para configurar uma política de retenção diferente, desmarque esta opção e configure uma política diferente.

6. Na seção **Proteção adicional**, configure as opções a seguir para transferir e arquivar dados.

Dica: Ao especificar Proteção adicional, você está optando por criar uma cópia.

Nuvem

Selecione esta opção para transferir dados para o armazenamento em nuvem ou para um servidor do repositório.

Importante: Clicando em **Proteção adicional > Nuvem**, você cria uma cópia incremental dos dados para um sistema de armazenamento em nuvem ou para um Servidor IBM Spectrum Protect .

Os dados são submetidos a backup no servidor vSnap para proteção de curto prazo e, em seguida, transferidos para o armazenamento em nuvem ou servidor do repositório selecionado para proteção de longo prazo. Durante a primeira transferência de um volume de backup, a captura instantânea é submetida a um backup completo. Após a conclusão da primeira transferência da captura instantânea de base, as transferências subsequentes são incrementais e capturam mudanças acumulativas desde a última transferência. As operações de restauração do servidor em nuvem ou de repositório podem ser executadas a partir de qualquer servidor vSnap disponível.

Desativar Programação

Selecione esta caixa de seleção para criar o relacionamento de transferência sem definir uma frequência ou horário de início.

Frequência

Insira uma frequência para operações de transferência.

Start Time

Insira a data e hora em que você deseja que a operação de transferência seja iniciada.

Mesma retenção que a seleção de origem

Selecione esta opção para usar a mesma política de retenção para o backup de transferência em nuvem que o servidor vSnap de origem. Para configurar uma política de retenção diferente, desmarque esta opção e configure uma política diferente.

Restrição: As opções de retenção de transferência serão desativadas se um servidor que usa a retenção write once read many (WORM) estiver selecionado no campo **Servidor de transferência de destino**.

Origem

Clique na origem para a operação de transferência:

Destino da Política Principal

A origem para a operação de transferência é o site de destino que está definido na seção **Política principal**.

Destino da Política de Replicação

A origem para a operação de transferência é o site de destino que está definido na seção **Política de replicação**.

Essa opção estará disponível somente quando **Replicação de armazenamento de backup** for selecionada.

Destination

Clique em **Servidores em Nuvem** ou **Servidores de Repositório**.

Resposta

Clique no sistema de armazenamento em nuvem ou no servidor do repositório para o qual você deseja transferir dados.

Essa lista contém os sistemas de armazenamento secundário que você incluiu no IBM Spectrum Protect Plus.. Se você não tiver incluído o armazenamento secundário ou desejar incluí-lo, consulte [“Gerenciando o armazenamento de backup secundário”](#) na página 257 para obter informações sobre os sistemas de armazenamento em nuvem e os servidores de repositório que são suportados e como incluí-los no IBM Spectrum Protect Plus.

Archive

Selecione essa opção para arquivar dados no armazenamento em nuvem ou em um servidor do repositório para proteção de longo prazo.

Importante: Clicando em **Proteção adicional > Archive**, você cria uma cópia completa dos dados para um sistema de armazenamento em nuvem ou para a fita usando um Servidor IBM Spectrum Protect.

Esta operação fornece uma transferência de imagem completa para o armazenamento de arquivamento selecionado.

Desativar Programação

Marque essa caixa de seleção para criar o relacionamento de archive sem definir uma frequência ou um horário de início.

Frequência

Insira uma frequência para operações de archive.

Start Time

Insira a data e hora em que você deseja que a operação de archive seja iniciada.

Retenção

Especifique o período de retenção para as capturas instantâneas de archive como uma unidade de tempo em dias, meses ou anos.

Origem

Clique na origem para o destino do archive:

Destino da Política Principal

A origem para a operação de archive é o site de destino que está definido na seção **Política principal**.

Destino da Política de Replicação

A origem para a operação de archive é o site de destino que está definido na seção **Política de replicação**.

Essa opção estará disponível somente quando **Replicação de armazenamento de backup** for selecionada.

Destination

Clique em **Servidores em Nuvem** ou **Servidores de Repositório**.

Resposta

Clique no sistema de armazenamento em nuvem ou no servidor do repositório no qual você deseja arquivar dados.

Somente os destinos em nuvem que têm um depósito de archive definido são mostrados nessa lista. Para incluir um depósito de archive para um sistema de armazenamento em nuvem, siga as instruções em [“Gerenciando o armazenamento em”](#) na página 257.

7. Clique em **Salvar**. A política de ANS agora pode ser aplicada a definições de tarefa de backup.

O que Fazer Depois

Depois de criar uma política de ANS, conclua as seguintes ações:

Ação	Como
Designe permissões de usuário à política de ANS.	Consulte “Criando uma função” na página 302
Crie uma definição de tarefa de backup que use a política de ANS.	Consulte os tópicos de backup em Capítulo 7, “Protegendo hypervisors” , na página 95 e Capítulo 8, “Protegendo Aplicativos” , na página 137.

Conceitos relacionados

[“Replicar dados de armazenamento de backup”](#) na página 5

Ao ativar a replicação de dados de backup, os dados de um servidor vSnap são replicados de forma assíncrona para outro servidor vSnap. Por exemplo, é possível replicar dados de backup de um servidor vSnap em um site primário para um servidor vSnap em um site secundário.

[“Transfload para armazenamento de backup secundário”](#) na página 6

O servidor vSnap é o local de backup primário para capturas instantâneas. Todos os ambientes do IBM Spectrum Protect Plus têm pelo menos um servidor vSnap. Opcionalmente, é possível transferir capturas instantâneas de um servidor vSnap para o armazenamento de backup secundário.

Editando uma política de SLA

Edite as opções para uma política de ANS para refletir mudanças no ambiente IBM Spectrum Protect Plus.

Procedimento

Para editar uma política de ANS, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Visão geral de política**.
2. Clique no ícone editar  que está associado a uma política.
A área de janela **Editar política de ANS** é exibida.
3. Edite as opções de política e, em seguida, clique em **Salvar**.

Excluindo uma política de SLA

Exclua uma política de ANS quando ela se tornar obsoleta.

Antes de Iniciar

Certifique-se de que não haja tarefas associadas à política de ANS.

Procedimento

Para excluir uma política de ANS, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Visão geral de política**.
2. Clique no ícone excluir  que está associado a uma política de ANS.
3. Clique em **Sim** para excluir a política.

4. Se estiver excluindo a política de demo de SLA, acesse **Configuração do sistema > Site** e exclua o site denominado Demo.

Nota:

Ao excluir o site de demonstração, deve-se registrar o vSnap do host local com as credenciais do usuário em outro site válido.

Capítulo 7. Protegendo hypervisors

Deve-se registrar os hypervisors que você deseja proteger no IBM Spectrum Protect Plus e, em seguida, criar tarefas para fazer backup e restaurar as máquinas virtuais e os recursos que estão associados aos hypervisors.

Fazendo Backup e Restaurando Dados do VMware

Para proteger dados do VMware, primeiro inclua instâncias do vCenter Server no IBM Spectrum Protect Plus e, em seguida, crie tarefas para operações de backup e restauração para o conteúdo das instâncias.

Requisitos de Sistema

Certifique-se de que o ambiente VMware atenda aos requisitos do sistema em [“Requisitos do Hypervisor”](#) na página 23.

Suporte para tags VMware

IBM Spectrum Protect Plus suporta tags da máquina virtual VMware. As tags são aplicadas no vSphere e permitem que os usuários designem metadados a máquinas virtuais. Quando aplicadas no vSphere e incluídas no inventário do IBM Spectrum Protect Plus, as tags de máquina virtual podem ser visualizadas por meio do filtro **Visualizar > Tags e Categorias** ao criar uma definição de tarefa. Para obter informações adicionais sobre tags do VMware, consulte [Identificando Objetos](#).

Suporte para criptografia

O backup e a restauração de máquinas virtuais criptografadas são suportados em ambientes vSphere 6.5 e mais recentes. As máquinas virtuais criptografadas podem ser submetidas a backup e restauradas no nível de máquina virtual para seu local original. Se estiver restaurando para um local alternativo, a máquina virtual criptografada será restaurada sem criptografia e deve ser criptografada manualmente por meio do vCenter Server após a conclusão da restauração.

Os seguintes privilégios do vCenter Server são necessários para ativar operações para máquinas virtuais criptografadas:

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

Incluindo uma Instância do vCenter Server

Quando uma instância do vCenter Server é incluída no IBM Spectrum Protect Plus, um inventário da instância é capturado, permitindo concluir tarefas de backup e restauração, bem como executar relatórios.

Procedimento

Para incluir uma instância do vCenter Server, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Clique em **Gerenciar vCenter**.
3. Clique em **Incluir vCenter**.
4. Preencha os campos na seção **Propriedades do vCenter**:

Hostname/IP

Insira o endereço IP resolvível ou um caminho e nome de máquina resolvíveis.

Usar usuário existente

Ative para selecionar um nome do usuário e senha inseridos anteriormente para a instância do vCenter Server.

Nome de Usuário

Insira seu nome de usuário para a instância do vCenter Server.

Password

Insira sua senha para a instância do vCenter Server.

Porta

Insira a porta de comunicações da instância do vCenter Server. Selecione a caixa de seleção **Usar SSL** para ativar uma conexão Secure Sockets Layer (SSL) criptografada. A porta padrão típica é 80 para conexões não SSL ou 443 para conexões SSL.

5. Na seção **Opções**, configure a seguinte opção:

Número máximo de VMs a serem processadas simultaneamente por servidor ESX e por ANS

Configure o número máximo de capturas instantâneas da VM simultâneas a serem processadas no servidor ESX.

6. Clique em **Salvar**. O IBM Spectrum Protect Plus confirma uma conexão de rede, inclui a instância do vCenter Server no banco de dados e, em seguida, cataloga a instância.

Se aparecer uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se suas entradas estiverem corretas e a conexão for malsucedida, entre em contato com um administrador da rede para revisar as conexões.

O que Fazer Depois

Depois de incluir uma instância do vCenter Server, conclua a seguinte ação:

Ação	Como
Designar permissões de usuário para o hypervisor.	Consulte “Criando uma função” na página 302.

Conceitos relacionados

[“Gerenciando identidades”](#) na página 307

Alguns recursos no IBM Spectrum Protect Plus requerem credenciais para acessar seus recursos. Por exemplo, o IBM Spectrum Protect Plus se conecta a servidores Oracle como o usuário do sistema operacional local que é especificado durante o registro para concluir tarefas, como catalogar, proteção de dados e restauração de dados.

Tarefas relacionadas

[“Fazendo backup dos dados de VMware”](#) na página 103

Use uma tarefa de backup para fazer backup de recursos do VMware, como máquinas virtuais, armazenamentos de dados, pastas, vApps e data centers com capturas instantâneas.

[“Restaurando Dados do VMware”](#) na página 111

As tarefas de restauração do VMware suportam cenários de Restauração de VM instantânea e de Restauração de disco instantâneo, que são criados com base na origem selecionada.

Privilégios de máquina

Privilégios do vCenter Server são necessários para as máquinas virtuais que estão associadas a um provedor VMware. Esses privilégios são incluídos na função de Administrador do vCenter.

Se o usuário que está associado ao provedor não estiver designado à função de Administrador para um objeto de inventário, o usuário deverá ser designado a uma função que tenha os seguintes privilégios necessários. Certifique-se de que os privilégios sejam propagados para objetos-filhos. Para obter instruções, consulte a documentação do VMware sobre como incluir uma permissão em um objeto de inventário.

Objeto do vCenter Server	Privilégios Necessários
Alarme	<ul style="list-style-type: none"> • Alarme de conhecimento • Definir status do alarme
Operações Criptográficas	<ul style="list-style-type: none"> • Incluir discos • Acesso direto • Criptografar • Criptografar novo • Gerenciar políticas de criptografia
Data Center	<ul style="list-style-type: none"> • Criar datacenter • Reconfigurar datacenter
Armazenamento de dados	<ul style="list-style-type: none"> • Alocar espaço • Procurar armazenamento de dados • Configurar armazenamento de dados • Operações de arquivo de baixo nível • Remover o arquivo • Atualizar arquivos da máquina virtual
Cluster de Armazenamento de Dados	<ul style="list-style-type: none"> • Configurar um cluster de armazenamento de dados
Comutador Distribuído	<ul style="list-style-type: none"> • Criar • Excluir • Operação do host • Modificar • Movimentação • Operação de Controle de E/S da Rede • Política de operação • Opção de configuração da • Operação de configuração de porta • Operação VSPAN
Gerenciador de Agentes ESX	<ul style="list-style-type: none"> • Config. • Modificar • Exibir
Ramal	<ul style="list-style-type: none"> • Registrar extensão
Pasta	<ul style="list-style-type: none"> • Criar pasta • Excluir pasta • Mover pasta • Renomear pasta

Objeto do vCenter Server	Privilégios Necessários
Global	<ul style="list-style-type: none"> • Cancelar tarefa • Diagnósticos (usados para resolução de problemas, não necessário para operações) • Desativar métodos • Ativar métodos • Licenças • Evento de log • Gerenciar atributos customizados • Configurar atributo customizado • Configurações
Host > Configuração	<ul style="list-style-type: none"> • Configurações avançadas • Configuração da partição de armazenamento
Serviço de Inventário > VSphere Tagging	<ul style="list-style-type: none"> • Designar ou Remover Designação da Tag do vSphere • Criar Tag do vSphere • Criar Categoria de Tag do vSphere • Modificar Campo UsedBy para a Categoria • Modificar Campo UsedBy para a Tag
Rede	<ul style="list-style-type: none"> • Designar rede • Configurar • Mover rede • Remover
Recurso	<ul style="list-style-type: none"> • Aplicar recomendação • Designar um vApp para o conjunto de recursos • Designar máquina virtual para o conjunto de recursos • Criar conjunto de recursos • Migrar VM Desligada • Migrar energia na VM • Modificar conjunto de recursos • Mover conjunto de recursos • Query vMotion • Remover conjunto de recursos • Renomear conjunto de recursos
Sessões	<ul style="list-style-type: none"> • Visualizar e parar sessões
Visualizações de armazenamento	<ul style="list-style-type: none"> • Configurar serviço • Exibir

Objeto do vCenter Server	Privilégios Necessários
Tarefas	<ul style="list-style-type: none"> • Criar tarefa • Tarefa de atualização
Máquina Virtual > Configuração	<ul style="list-style-type: none"> • Incluir disco existente • Incluir novo disco • Incluir ou remover dispositivo • Avançada • Mudar contagem de CPUs • Alterar recurso • Configurar managedBy • Rastreamento de mudança de • Lease de disco • Exibir Configurações de Conexão • Estender disco virtual • Dispositivo USB do host • do NT • Modificar configurações do dispositivo • Compatibilidade de Tolerância de Falhas de • Consultar arquivos sem proprietário • Dispositivo bruto • Recarregar a partir do caminho • Remover o disco (desconectar e remover o disco virtual) • Renomear • Reconfigurar informações do convidado • Configurar anotação • Configurações • Posicionamento do Swapfile • Desbloquear a máquina virtual • Compatibilidade da máquina virtual de
Máquina Virtual > Operações Guest	<ul style="list-style-type: none"> • Modificações da Operação Guest • Execução do Programa Guest Operation • Consultas de operação da máquina guest

Objeto do vCenter Server	Privilégios Necessários
Máquina Virtual > Interação	<ul style="list-style-type: none"> • Pergunta de resposta • Operação de backup na máquina virtual • Configurar mídia de CD • Configurar Mídia de Floppy • Interação do console • Criar captura de tela • Desfragmentar todos os discos • Conexão de dispositivo • Desativar Tolerância de Falhas • Ativar tolerância a falhas • Gerenciamento de sistema operacional guest pela API VIX • Injetar códigos de varredura do HID USB • Executar operações de limpeza ou de redução • Desligar • Ativado Ligado • Gravar sessão na VM • Reproduzir sessão na VM • Reconfigurar • Retomar Tolerância a Falhas • Suspende • Suspende Tolerância a Falhas • Failover de teste • Teste de reinicialização da VM Secund • Desativar tolerância a falhas • Ligar Tolerância a Falhas • Instalação do VMware Tools
Máquina Virtual > Inventário	<ul style="list-style-type: none"> • Criar a partir de existentes • Criar Novo • Movimentação • Registrar • Remover • Cancelar Registro

Objeto do vCenter Server	Privilégios Necessários
Máquina Virtual > Fornecimento	<ul style="list-style-type: none"> • Permitir acesso ao disco • Permitir acesso ao disco somente leitura • Permitir download da máquina virtual • Permitir upload de arquivos da máquina virtual • Clonar modelo • Clonar máquina virtual • Criar modelo a partir da máquina virtual • Customizar • Implementar modelo • Marcar como modelo • Marcar como máquina virtual • Modificar a especificação de customização • Promover discos • Ler especificações de customização
Máquina Virtual > Configuração de Serviço	<ul style="list-style-type: none"> • Permitir notificações • Permitir polling de notificações de eventos globais • Gerenciar configurações de serviço • Modificar configurações de serviço • Consultar Configurações de Serviço • Ler configurações de serviço
Máquina Virtual > Gerenciamento de Captura Instant	<ul style="list-style-type: none"> • Criar captura instantânea • Remover captura instantânea • Renomear captura instantânea • Reverter para a captura instantânea
Máquina Virtual > Replicação do vSphere	<ul style="list-style-type: none"> • Configurar replicação • Gerenciar replicação • Monitorar a replicação

Objeto do vCenter Server	Privilégios Necessários
vApp	<ul style="list-style-type: none"> • Incluir VM no vApp • Designar conjunto de recursos ao vApp • Designar vApp para outro vApp • Clonar • Criar • Excluir • Exportar • Importe o certificado raiz • Movimentação • Desligar • Ativado Ligado • Renomear • Suspende • Cancelar Registro • Visualizar Ambiente OVF • Configuração do Aplicativo vApp • Configuração da instância do vApp • Configuração do vApp managedBy • Configuração de recurso do vApp

Detectando Recursos do VMware

Os recursos do VMware são detectados automaticamente após a instância do vCenter Server ser incluída no IBM Spectrum Protect Plus. No entanto, é possível executar uma tarefa de inventário para detectar quaisquer mudanças que ocorreram desde que a instância foi incluída.

Procedimento

Para executar uma tarefa de inventário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Na lista de instâncias do vCenters Server, selecione uma instância ou clique no link para a instância para navegar para o recurso desejado. Por exemplo, se desejar executar uma tarefa de inventário para uma máquina virtual individual na instância, clique no link de instância e, em seguida, selecione uma máquina virtual.
3. Clique em **Executar Inventário**.

Testando a conexão com uma máquina virtual vCenter Server

É possível testar a conexão com uma máquina virtual do vCenter Server. A função de teste verifica a comunicação com a máquina virtual e testa as configurações do servidor de nomes de domínio (DNS) entre o dispositivo virtual IBM Spectrum Protect e a máquina virtual.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Na lista de instâncias do vCenters Server, clique no link para um vCenter Server para navegar para as máquinas virtuais individuais.
3. Selecione uma máquina virtual e, em seguida, clique em **Selecionar opções**.
4. Selecione **Usar usuário existente**.

5. Selecione um usuário na lista **Selecionar usuário**.
6. Clique em **Testar**.

Fazendo backup dos dados de VMware

Use uma tarefa de backup para fazer backup de recursos do VMware, como máquinas virtuais, armazenamentos de dados, pastas, vApps e data centers com capturas instantâneas.

Antes de Iniciar

Revise os seguintes procedimentos e considerações antes de criar uma definição de tarefa de backup:

- Registre os provedores dos quais você deseja fazer backup. Para obter mais instruções, consulte [“Incluindo uma Instância do vCenter Server”](#) na página 95.
- Configure políticas do SLA. Para obter mais instruções, consulte [“Criar políticas de backup”](#) na página 73.
- Antes de um usuário do IBM Spectrum Protect Plus poder implementar operações de backup e restauração, as funções devem ser designadas ao usuário. Conceda aos usuários acesso a hypervisors e a operações de backup e restauração usando a área de janela **Contas**. As funções e permissões associadas são designadas durante a criação da conta do usuário. Para obter mais informações, consulte Capítulo 13, [“Gerenciando o acesso de”](#), na página 297 e [“Gerenciando contas do usuário”](#) na página 305.
- Se uma máquina virtual estiver associada a várias políticas de ANS, certifique-se de que as políticas não sejam planejadas para execução simultaneamente. Planeje as políticas de ANS para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de ANS.
- Se seu vCenter for uma máquina virtual, para ajudar a aumentar a proteção de dados, deixe o vCenter em um armazenamento de dados dedicado e submetido a backup em uma tarefa de backup separada.
- Ao fazer backup de máquinas virtuais VMware, o IBM Spectrum Protect Plus faz download de arquivos .vmx, .vmxf e .nvram, se necessário e, em seguida, transfere esses arquivos para o vSnap conforme necessário. Para que isso funcione com sucesso, o dispositivo IBM Spectrum Protect Plus deve poder resolver e acessar todos os hosts ESXi protegidos; e ao comunicar-se com um host ESXi, o endereço IP correto deve ser retornado.
- Se uma VM for protegida por uma política de ANS, os backups da VM serão retidos com base nos parâmetros de retenção da política de ANS, mesmo se a VM for removida do vCenter.
- Em alguns casos, as tarefas de backup do VMware falham com erros de “falha ao montar”. Para resolver este problema, aumente o número máximo de montagens de NFS para pelo menos 64 usando os valores NFS.MaxVolumes (vSphere 5.5 e mais recente) e NFS41.MaxVolumes (vSphere 6.0 e mais recente). Siga as instruções em [Aumentando o valor padrão que define o número máximo de montagens NFS em um host ESXi/ESX](#).
- Se uma VM existente for submetida ao vMotion, o IBM Spectrum Protect Plus executará uma nova base, se necessário.

Procedimento

Para definir uma tarefa de backup do VMware, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Selecione os recursos para fazer backup.
Use a função de procura para procurar recursos disponíveis e alternar os recursos exibidos usando o filtro **Visualizar**. As opções disponíveis são **MVs e modelos, MVs, Armazenamento de dados, Tags e categoriase Hosts e clusters**. As tags são aplicadas no vSphere e permitem que um usuário designe metadados a máquinas virtuais.
3. Clique em **Selecionar política de ANS** para incluir uma ou mais políticas de ANS que atendem aos critérios de dados de backup para a definição de tarefa.
4. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.

A tarefa é executada conforme definido pelas políticas de SLA selecionadas. Para executar a tarefa manualmente, clique em **Tarefas e operações > Planejamento**. Selecione a tarefa e clique em **Ações > Iniciar**.

Dica: o botão **Executar** é ativado somente para um único backup de hypervisor e o hypervisor deve ter uma política de ANS aplicada.

Quando a definição de tarefa é salva, os discos de máquina virtual (VMDKs) disponíveis em uma máquina virtual são descobertos e mostrados quando a opção **VMs e modelos** é selecionada no filtro **Visualização**. Por padrão, esses VMDKs são designados à mesma política de ANS que a máquina virtual. Se desejar uma operação de backup mais granular, será possível excluir VMDKs individuais da política de ANS. Para obter instruções, consulte [“Excluindo VMDKs da política de ANS para uma tarefa” na página 107](#).

5. Para editar opções antes de criar a definição de tarefa, clique em **Selecionar opções**.

Na seção **Opções de backup**, configure as seguintes opções de definição de tarefa:

Ignorar armazenamentos de dados somente leitura

Ignore armazenamentos de dados que são montados como somente leitura.

Ignorar armazenamentos de dados temporários montados para acesso instantâneo

Exclua armazenamentos de dados de Acesso instantâneo temporário da definição de tarefa de backup.

Proxy VADP

Selecione um proxy VADP para balancear a carga.

Prioridade

Configure a prioridade de backup do recurso selecionado. Os recursos com uma configuração de prioridade mais alta são submetidos a backup primeiro na tarefa. Clique no recurso que você deseja priorizar na seção **Backup do VMware** e, em seguida, configure a prioridade de backup no campo **Prioridade**. Configure 1 para o recurso de prioridade mais alta ou 10 para a mais baixa. Quando um valor de prioridade não é configurado, a opção designa automaticamente uma prioridade de 5 é configurada por padrão.

Na seção **Opções de captura instantânea**, configure as seguintes opções de definição de tarefa:

Tornar o aplicativo/sistema de arquivos de captura instantânea da VM consistente

Ative esta opção para ativar a consistência do aplicativo ou do sistema de arquivos para a captura instantânea de máquina virtual. Todos os aplicativos compatíveis com VSS, como Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL e o estado do sistema são colocados em modo quiesce. Os VMDKs e as máquinas virtuais podem ser montados instantaneamente para restaurar dados que estão relacionados a aplicativos em modo quiesce.

Tentativas de nova tentativa de captura instantânea da VM

Configure o número de vezes que o IBM Spectrum Protect Plus tenta capturar uma captura instantânea consistente de aplicativo ou de arquivo de uma máquina virtual antes do cancelamento da tarefa. Se a opção **Voltar para captura instantânea retirada do modo quiesce se a captura instantânea em modo quiesce falhar** estiver ativada, será obtida uma captura instantânea retirada do modo quiesce após a nova tentativa.

Voltar para captura instantânea retirada do modo quiesce se a captura instantânea em modo quiesce falhar

Ative para voltar para uma captura instantânea consistente não de aplicativo ou não de sistema de arquivos se a captura instantânea consistente de aplicativo falhar. Selecionar esta opção assegura que uma será obtida uma captura instantânea retirada do modo quiesce, se problemas ambientais proibirem a captura de uma captura instantânea consistente de aplicativo ou de sistema de arquivos.

Na seção **Opções do agente**, configure as seguintes opções de definição de tarefa:

Truncate os logs SQL

Para truncar logs do aplicativo para o SQL Server durante a tarefa de backup, ative a opção **Truncar logs de SQL**. As credenciais devem ser estabelecidas para a máquina virtual associada usando as opções Nome do usuário de S.O. guest e Senha de S.O. guest na definição de tarefa de backup. Quando a máquina virtual está conectada a um domínio, a identidade do usuário segue o formato padrão *domain\name*. Se o usuário for um administrador local, o formato *local_administrator* será usado.

A identidade do usuário deve ter privilégios de administrador local. No servidor SQL Server, a credencial de logim do sistema deve ter as seguintes permissões:

- As permissões sysadmin do SQL Server devem estar ativadas.
- O direito **Efetuar logon como um serviço** deve ser configurado. Para obter informações adicionais sobre este direito, consulte [Incluir o direito Efetuar logon como um serviço em uma conta](#).

O IBM Spectrum Protect Plus gera arquivos de log para a função de truncamento do log e copia-os para o seguinte local no dispositivo IBM Spectrum Protect:

```
/data/log/guestdeployer/ latest_date / latest_entry / vm_name
```

Em que *latest_date* é a data em que ocorreu o truncamento da tarefa de backup e do log, *latest_entry* é o identificador exclusivo universal (UUID) para a tarefa e *vm_name* é o nome do host ou endereço IP da VM na qual ocorreu o truncamento do log.

Restrição: A indexação de arquivo e a restauração de arquivo não são suportadas a partir de pontos de restauração que foram transferidos para recursos em nuvem ou servidores do repositório.

Metadados do Arquivo de Catálogo

Ative a indexação de arquivo para a captura instantânea associada. Quando a indexação de arquivo estiver concluída, os arquivos individuais podem ser restaurados usando a área de janela **Restauração de arquivo** no IBM Spectrum Protect Plus. As credenciais devem ser estabelecidas para a máquina virtual associada usando uma chave SSH, ou as opções **Nome do usuário de S.O. guest** e **Senha de S.O. guest** na definição de tarefa de backup. Certifique-se de que a máquina virtual possa ser acessada a partir do dispositivo IBM Spectrum Protect Plus usando um nome de DNS ou de host.

Restrições: As chaves SSH não são um mecanismo de autorização válido para plataformas Windows.

A indexação de arquivo e a restauração de arquivo não são suportadas a partir de pontos de restauração que foram transferidos para recursos em nuvem ou servidores do repositório.

Arquivos de Exclusão

Insira diretórios a serem ignorados quando a indexação de arquivo for executada. Os arquivos nesses diretórios não são incluídos no catálogo do IBM Spectrum Protect Plus e não estão disponíveis para recuperação de arquivo. Os diretórios podem ser excluídos por meio de uma correspondência exata ou com asteriscos curinga especificados antes do padrão (*test) ou depois do padrão (test*). Vários curingas asteriscos também são suportados em um único padrão. Os padrões suportam caracteres alfanuméricos padrão, bem como os seguintes caracteres especiais: - _ e *. Separe vários filtros com um ponto-e-vírgula.

Usar usuário existente

Selecione um nome de usuário e uma senha inseridos anteriormente para o provedor.

Guest OS Username / Password

Para algumas tarefas (como catalogar metadados do arquivo, restauração de arquivo e reconfiguração de IP), as credenciais devem ser estabelecidas para a máquina virtual associada. Insira o nome do usuário e a senha e certifique-se de que a máquina virtual possa ser acessada a partir do dispositivo IBM Spectrum Protect Plus usando um nome de DNS ou do host.

6. Para resolver problemas de uma conexão com uma máquina virtual do hypervisor, use a função **Testar**.

A função **Testar** verifica a comunicação com a máquina virtual e testa configurações de DNS entre o dispositivo IBM Spectrum Protect Plus e a máquina virtual. Para testar uma conexão, selecione uma única máquina virtual, em seguida, clique em **Selecionar opções**. Selecione **Usar usuário existente** e

selecione um nome de usuário e senha inseridos anteriormente para o recurso. O botão **Testar** é exibido à direita do botão **Salvar** na seção **Opções**. Clique em **Testar**.

7. Clique em **Salvar**.

8. Para configurar opções adicionais, clique no campo **Opções de política** que está associado à tarefa na seção **Status de política de ANS**. Configure as opções de política adicionais:

Pré-scripts e pós-scripts

Execute um pré-script ou um post-script. Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de uma tarefa. As máquinas baseadas no Windows suportam scripts de Lote e PowerShell enquanto as máquinas baseadas no Linux suportam shell scripts.

Na seção **Pré-script** ou **Pós-script**, selecione um script transferido por upload e um servidor de script no qual o script será executado. Os scripts e servidores de script podem ser configurados usando a página **Configuração do sistema > Script**.

Para continuar executando a tarefa se o script associado à tarefa falhar, selecione **Continuar a tarefa durante erro do script**.

Quando esta opção é ativada, se um pré-script ou pós-script concluir o processamento com um código de retorno diferente de zero, será feita uma tentativa de operação de backup ou de restauração e o status da tarefa de pré-script será relatado como CONCLUÍDO. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa de pós-script será relatado como CONCLUÍDO.

Quando esta opção é desativada, não é feita tentativa de backup ou de restauração e o status da tarefa de pré-script ou pós-script é relatado como COM FALHA.

Executar inventário antes do backup

Execute uma tarefa de inventário e capture os dados mais recentes dos recursos selecionados antes de iniciar a tarefa de backup.

Recursos de Exclusão

Exclua recursos específicos da tarefa de backup usando padrões de exclusão únicos ou múltiplos. Os recursos podem ser excluídos usando uma correspondência exata ou com asteriscos curinga especificados antes do padrão (*test) ou depois do padrão (test*).

Vários curingas asteriscos também são suportados em um único padrão. Os padrões suportam caracteres alfanuméricos padrão, bem como os seguintes caracteres especiais: - _ e *.

Separe vários filtros com um ponto-e-vírgula.

Forçar Backup Completo de Recursos

Forçar operações de backup de base para máquinas virtuais ou bancos de dados específicos na definição da tarefa de backup. Separe vários recursos com um ponto-e-vírgula.

9. Para salvar as opções adicionais configuradas, clique em **Salvar**.

O que Fazer Depois

Depois de definir uma tarefa de backup, é possível concluir as seguintes ações:

Ação	Como
Se estiver usando um ambiente Linux, considere a criação de proxies VADP para ativar o compartilhamento de carregamento.	Consulte “Criando proxies do VADP” na página 108.
Crie uma definição de tarefa de restauração do VMware.	Consulte “Restaurando Dados do VMware” na página 111.

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração”](#) na página 255

Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de tarefas de backup e restauração no nível de tarefa. Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts são criados localmente, transferidos por upload para seu ambiente por meio da página **Script** e, em seguida, aplicados a definições de tarefa.

Tarefas relacionadas

“Iniciando Tarefas” na página 252

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Excluindo VMDKs da política de ANS para uma tarefa

Depois de salvar uma definição de tarefa de backup, é possível excluir VMDKs individuais em uma máquina virtual a partir da política de ANS que está designada à tarefa.

Procedimento

Para excluir VMDKs da política de ANS:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Selecione **VMs e modelos** no filtro **Visualização**.
3. Clique no link para o vCenter e, em seguida, clique no link para a máquina virtual que contém os VMDKs que você deseja excluir.
4. Selecione um ou mais VMDKs e, em seguida, clique em **Selecionar política de ANS**.
5. Desmarque a caixa de seleção para a política de ANS selecionada e, em seguida, clique em **Salvar**.

Fazendo backup de um vCenter Server Appliance baseado no Linux

Para fazer backup de um dispositivo vCenter Server baseado no Linux, deve-se modificar os scripts de pré-congelamento e de pós-descongelamento do VMware na máquina virtual vCenter para evitar backups do vCenter corrompidos.

Procedimento

Para modificar os scripts, conclua as seguintes etapas:

1. Na máquina virtual, navegue para o diretório `/usr/sbin` e substitua o conteúdo do script `pre-freeze-script` pelo seguinte conteúdo:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log "
#set and log start date
today=`date +%Y %m %d %H: %M: %S `
echo "${today}: Start of creation consistent state" >> ${log}
comando #execute freeze
cmd="echo \"SELECT pg_start_backup('${today}', true);\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log}
2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y %m %d %H: %M: %S `
echo "${today}: Finished freeze script" >> ${log}
```

2. Substitua o conteúdo do script `post-thaw-script` pelo seguinte conteúdo:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log "
#set and log start date
today=`date +%Y %m %d %H: %M: %S `
echo "${today}: Release of backup" >> ${log}
#execute release command
cmd="echo \"SELECT pg_stop_backup();\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log} 2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y %m %d %H: %M: %S `
echo "${today}: Finished thaw script" >> ${log}
```

Gerenciando proxies de backup do VADP

No IBM Spectrum Protect Plus, é possível criar proxies para executar tarefas de backup do VMware usando o vStorage API for Data Protection (VADP) em ambientes Linux. Os proxies reduzem a demanda de recursos do sistema ativando o compartilhamento de carga e o balanceamento de carga. A limitação

assegura que vários proxies VADP sejam utilizados de forma ideal para aumentar o rendimento de dados. Para cada máquina virtual que está sendo submetida a backup, o IBM Spectrum Protect Plus determina qual proxy VADP é o menos ocupado e tem a maior quantidade de memória disponível e de tarefas livres. As tarefas livres são determinadas pelo número de núcleos da CPU disponíveis ou usando a opção **Limite leve de tarefas**.

Certifique-se de que tenha as permissões de usuário necessárias para trabalhar com proxies VADP. Para obter instruções sobre como gerenciar permissões de proxy VADP, consulte [“Tipos de Permissão”](#) na página 303.

O backup de uma máquina virtual VMware inclui os seguintes arquivos:

- VMDKs correspondentes a todos os discos. O backup de base captura todos os dados alocados ou todos os dados se os discos estiverem em armazenamentos de dados NFS. Os backups incrementais irão capturar somente blocos alterados desde o último backup bem-sucedido.
- Modelos de máquina virtual
- Arquivos do VMware com as seguintes extensões:
 - .vmx
 - .vmfx (se disponível)
 - .nvram (armazena o estado do BIOS da máquina virtual)

Se existirem proxies, toda a carga de processamento será desativada do sistema host e nos proxies. Se os proxies não existirem, a carga inteira permanecerá no host. A limitação assegura que vários proxies VADP sejam utilizados de forma ideal para aumentar o rendimento de dados. Para cada máquina virtual que está sendo submetida a backup, o IBM Spectrum Protect Plus determina qual proxy VADP é o menos ocupado e tem a maior quantidade de memória disponível e tarefas livres.

Se um servidor proxy ficar inativo ou, de outra forma, ficar indisponível antes do início da tarefa, os outros proxies assumirão o controle e a tarefa será concluída. Se não existirem outros proxies, o host assumirá o controle da tarefa. Se um servidor proxy se tornar indisponível quando uma tarefa estiver em execução, a tarefa poderá falhar.

Os modos de transporte descrevem o método pelo qual um proxy VADP move dados. O modo de transporte é configurado como uma propriedade do proxy. A maioria das tarefas de backup e de recuperação é configurada posteriormente para usar um ou mais proxies.

Os proxies VADP no IBM Spectrum Protect Plus suportam os seguintes modos de transporte do VMware: SAN, HotAdd, NBDSSL e NBD.

Embora cada empresa seja diferente, e as prioridades em termos de tamanho, velocidade, confiabilidade e complexidade variem de ambiente para ambiente, as seguintes diretrizes gerais se aplicam à seleção de Modo de transporte:

- O modo de transporte SAN deve ser usado em um ambiente de armazenamento direto, porque esse modo é rápido e geralmente confiável.
- O modo de transporte HotAdd deve ser usado se o proxy VADP for virtualizado. Esse modo suporta todos os tipos de armazenamento do vSphere.
- Modo de transporte NBD ou NBDSSL (LAN) é o modo de fallback porque funciona em ambientes físicos, virtuais e mistos. No entanto, com este modo, a velocidade de transferência de dados pode ficar comprometida se as conexões de rede forem lentas. O modo NBDSSL é semelhante ao modo NBD, exceto que os dados transferidos entre o proxy VADP e o servidor ESXi são criptografados usando NBDSSL.

Criando proxies do VADP

É possível criar proxies VADP para executar tarefas de backup do VMware com o IBM Spectrum Protect Plus em ambientes Linux.

Antes de Iniciar

Observe as seguintes considerações antes de criar proxies VADP:

- Revise os requisitos do sistema IBM Spectrum Protect Plus em [“Requisitos do proxy do VADP”](#) na página 17.
- A versão do IBM Spectrum Protect Plus do instalador do proxy VADP inclui o Virtual Disk Development Kit (VDDK) versão 6.5. Esta versão do instalador do proxy VADP fornece o suporte de proxy VADP externo com o vSphere 6.5.

Procedimento

Para criar proxies VMware VADP, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Proxy VADP**.
2. Clique em **Registrar Proxy**.
3. Preencha os seguintes campos na área de janela **Instalar proxy VADP**:

Hostname/IP

Insira o endereço IP resolvível ou um caminho e nome de máquina resolvíveis.

Selecionar um site

Selecione um site para associar ao proxy.

Utilizar usuário existente

Ative para selecionar um nome do usuário e senha inseridos anteriormente para o provedor.

Nome de Usuário

Insira o nome do usuário para o servidor proxy VADP.

Password

Insira o nome da senha para o servidor proxy VADP.

4. Clique em **Instalar**.

O proxy é incluído na tabela **Proxy VADP**.

5. Clique em **Registrar** para registrar o servidor proxy.

É possível cancelar o registro ou suspender o servidor usando o menu **Ações**. A suspensão de um proxy impede que tarefas de backup futuras usem o proxy, e as tarefas que usam um proxy suspenso ou não registrado serão executadas localmente, o que pode afetar o desempenho. É possível concluir tarefas de manutenção no proxy enquanto ele estiver suspenso. Para continuar o uso do proxy, selecione **Ações > Continuar**.

Após o registro bem-sucedido, o serviço vadv é iniciado na máquina proxy. Um arquivo de log vadv.log é gerado no diretório /opt/IBM/SPP/logs.

6. Repita as etapas anteriores para cada proxy que você deseja criar.

A conexão entre o dispositivo virtual IBM Spectrum Protect Plus e um proxy VADP registrado é uma conexão bidirecional que requer que o dispositivo virtual IBM Spectrum Protect Plus tenha conectividade com o proxy VADP, e que o proxy VADP tenha conectividade com o dispositivo virtual IBM Spectrum Protect Plus. Para assegurar uma conexão adequada do dispositivo virtual IBM Spectrum Protect Plus com o proxy VADP, verifique se o dispositivo virtual IBM Spectrum Protect Plus pode executar ping para o proxy VADP concluindo as seguintes etapas:

1. Conecte-se à linha de comandos para o dispositivo virtual IBM Spectrum Protect Plus usando o protocolo de rede Shell Seguro (SSH).
2. Execute ping <vadv_ip>, em que <vadv_ip> é o endereço IP resolvível do proxy VADP.

Se o ping falhar, certifique-se de que o endereço IP do proxy VADP seja resolvível e endereçável pelo dispositivo IBM Spectrum Protect Plus e que exista uma rota do dispositivo IBM Spectrum Protect Plus para o proxy VADP. Se o ping for bem-sucedido, certifique-se de que haja uma conexão adequada do proxy VADP com o dispositivo virtual IBM Spectrum Protect Plus executando o seguinte procedimento:

1. Conecte-se à linha de comandos para o proxy VADP usando o protocolo de rede Shell Seguro (SSH).

2. Execute ping <spectrum_protect_plus_ip>, em que <spectrum_protect_plus_ip> é o endereço IP resolvível do dispositivo virtual IBM Spectrum Protect Plus.

Se o ping falhar, certifique-se de que o endereço IP do dispositivo virtual IBM Spectrum Protect Plus seja resolvível e endereçável pelo proxy VADP. Certifique-se de que exista uma rota do proxy VADP para o dispositivo virtual IBM Spectrum Protect Plus.

O que Fazer Depois

Depois de criar os proxies VADP, conclua a seguinte ação:

Ação	Como
Execute a tarefa de backup do VMware.	Consulte “Fazendo backup dos dados de VMware” na página 103. Os proxies são indicados no log da tarefa por uma mensagem de log semelhante ao seguinte texto: Run remote vmdkbackup of MicroService: http://<proxy> <i>nodename, IP:proxy_IP_address</i>

Tarefas relacionadas

[“Configurando Opções para Proxies VADP” na página 110](#)

É possível criar proxies VADP para executar tarefas de backup do VMware com o IBM Spectrum Protect Plus em ambientes Linux.

Configurando Opções para Proxies VADP

É possível criar proxies VADP para executar tarefas de backup do VMware com o IBM Spectrum Protect Plus em ambientes Linux.

Procedimento

Para configurar opções para proxies VMware VADP, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Proxy VADP**.
2. Clique no ícone de opções ******* para visualizar as opções disponíveis para o proxy.
3. Preencha os seguintes campos na área de janela **Configurar opções de proxy VADP**:

Site

Designe um site para o proxy.

Usuário

Selecione um nome de usuário inserido anteriormente para o provedor. Para ativar as atualizações automáticas do proxy VADP, um nome de usuário inserido anteriormente deve ser selecionado.

Modos de transporte

Configure os modos de transporte a serem usados pelo proxy. Para obter informações adicionais sobre modos de transporte do VMware, consulte [Métodos de transporte de disco virtual](#).

Ativar compactação NBDSSL

Se você selecionou o modo de transporte NBDSSL, ative a compactação para aumentar o desempenho de transferências de dados.

Para desativar a compactação, selecione **desativado**.

Retenção de log em dias

Configure o número de dias para reter os logs antes de serem excluídos.

Tamanho do buffer de leitura e gravação

Configure o tamanho do buffer da transferência de dados, medido em bytes.

Tamanho de bloco do volume NFS

Configure o tamanho do bloco a ser usado pelo volume NFS montado, medido em bytes.

Limite de tarefa do Softcap

Configure o número de VMs simultâneas que um proxy pode processar. Se a opção **Usar todos os recursos** estiver selecionada, o número de CPUs no proxy determinará o limite de tarefas com base na seguinte fórmula:

1 CPU = 1 VMDK

Uma CPU é a menor unidade de hardware capaz de executar um encadeamento. O número de CPUs em um proxy é determinado usando o comando `lscpu`.

O que Fazer Depois

Depois de criar os proxies VADP, conclua as seguintes ações:

Ação	Como
Execute a tarefa de backup do VMware.	Consulte “Fazendo backup dos dados de VMware” na página 103 . Os proxies são indicados no log da tarefa por uma mensagem de log semelhante ao seguinte texto: Executar vmdkbackup remoto de MicroService: <code>http://<proxy nodename, IP:proxy_IP_address</code>
Desinstale os proxies quando você deixar de executar as tarefas de backup do VMware.	Para desinstalar um proxy, execute o seguinte comando no sistema host a partir do subdiretório de desinstalação do diretório de instalação <code>/opt/IBM/SPP</code> : <code>./uninstall_vmdkbackup</code>

Tarefas relacionadas

“Criando proxies do VADP” na página 108

É possível criar proxies VADP para executar tarefas de backup do VMware com o IBM Spectrum Protect Plus em ambientes Linux.

Desinstalando proxies VADP

É possível remover proxies VADP do ambiente IBM Spectrum Protect Plus.

Procedimento

Para desinstalar proxies VADP do IBM Spectrum Protect Plus, conclua as seguintes etapas:

1. Em um prompt de comandos, navegue para o diretório `/opt/IBM/SPP/uninstall` no sistema host do proxy.
2. Execute o seguinte comando:
`./uninstall_vmdkbackup`

Restaurando Dados do VMware

As tarefas de restauração do VMware suportam cenários de Restauração de VM instantânea e de Restauração de disco instantâneo, que são criados com base na origem selecionada.

Antes de Iniciar

Execute as seguintes tarefas:

- Certifique-se de que uma tarefa de backup do VMware tenha sido executada pelo menos uma vez. Para obter instruções, consulte [“Fazendo backup dos dados de VMware”](#) na página 103.
- Antes de um usuário do IBM Spectrum Protect Plus poder concluir operações de backup e restauração, as funções devem ser designadas ao usuário. Conceda aos usuários acesso a hypervisors e a operações de backup e restauração por meio da área de janela **Contas**. As funções e permissões associadas são designadas durante a criação da conta do usuário. Para obter mais informações, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297 e [“Gerenciando contas do usuário”](#) na página 305.
- O tamanho de uma máquina virtual que é restaurada de uma transferência do vSnap para um ponto de restauração do IBM Spectrum Protect será igual ao tamanho thick provisioned da máquina virtual, independentemente do fornecimento de origem devido ao uso de armazenamentos de dados NFS durante a transferência. O tamanho padrão dos dados deve ser transferido, mesmo que não esteja alocado na máquina virtual de origem.
- Certifique-se de que o destino que você planeja usar para a tarefa de restauração esteja registrado no IBM Spectrum Protect Plus. Esse requisito se aplica às tarefas de restauração que restauram dados para hosts ou clusters originais.
- A indexação de arquivo e a restauração de arquivo do Windows em volumes que residem em discos dinâmicos não são suportadas.
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Sobre Esta Tarefa

Se um VMDK for selecionado para operação de restauração, o IBM Spectrum Protect Plus apresentará automaticamente opções para uma tarefa de restauração de Disco Instantâneo, que fornece acesso gravável instantâneo a pontos de restauração de dados e aplicativos. Uma captura instantânea do IBM Spectrum Protect Plus é mapeada para um servidor de destino, onde pode ser acessada ou copiada, conforme necessário.

Todas as outras origens são restauradas por meio de tarefas de restauração de VM instantâneas, que podem ser executadas nos seguintes modos:

Modo de teste

O modo de teste cria máquinas virtuais temporárias para desenvolvimento ou teste, verificação de captura instantânea e verificação de recuperação de desastre em uma base planejada e repetida, sem afetar os ambientes de produção. As máquinas de teste são mantidas em execução durante o tempo necessário para concluir o teste e a verificação e, em seguida, são limpas. Através da rede protegida, é possível estabelecer um ambiente seguro para testar suas tarefas sem interferir nas máquinas virtuais usadas para produção. As máquinas virtuais que são criadas no modo de teste também recebem nomes e identificadores exclusivos para evitar conflitos dentro de seu ambiente de produção. Para obter instruções para criar uma rede protegida, consulte [“Criando uma rede protegida por meio de uma tarefa de restauração do VMware”](#) na página 118.

Modo Clone

O modo Clone cria cópias de máquinas virtuais para casos de uso que requerem cópias permanentes ou de longa execução para mineração de dados ou duplicação de um ambiente de teste em uma rede protegida. As máquinas virtuais que são criadas no modo de clonagem também recebem nomes e identificadores exclusivos para evitar conflitos dentro de seu ambiente de produção. Com o modo clone, deve-se ficar atento ao consumo de recursos, pois esse modo cria máquinas virtuais permanentes ou de longo prazo.

Modo de produção

O modo de produção permite uma recuperação de desastre no site local, a partir do armazenamento primário ou em um site de recuperação de desastre remoto, substituindo imagens de máquina originais por imagens de recuperação. Todas as configurações são feitas como parte da recuperação,

incluindo nomes e identificadores, e todas as tarefas de cópia de dados associadas à máquina virtual continuam sendo executadas.

Procedimento

Para definir uma tarefa de restauração do VMware, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar tarefa de restauração > VMware**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, execute as ações a seguir:
 - a) Revise as origens disponíveis, incluindo máquinas virtuais (MVs) e discos virtuais (VDisks). Use o filtro **Visualizar** para alternar as origens exibidas para mostrar hosts e clusters, MVs ou tags e categorias. É possível expandir uma origem clicando em seu nome.

Também é possível inserir todo ou parte de um nome na caixa **Procurar** para localizar as MVs que correspondem aos critérios de procura. É possível utilizar o caractere curinga (*) para representar todo ou parte de um nome. Por exemplo, vm2* representa todos os recursos que começam com "vm2".
 - b) Clique no ícone de mais  ao lado do item que você deseja incluir na lista de restauração ao lado da lista de origens. É possível incluir mais de um item do mesmo tipo (MV ou disco virtual).

Para remover um item da lista de restauração, clique no ícone de menos  ao lado do item.
 - c) Clique em **Avançar**.
 3. Na página **Captura instantânea de origem**, especifique a instância da MV ou do disco virtual que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar. Alguns campos não são exibidos até que um campo relacionado seja selecionado.

Opção	Descrição
Tipo de Restauração	Selecione o tipo de tarefa de restauração: On Demand Executa uma operação de restauração única. Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.
Tipo de local da restauração	Selecione um tipo de local a partir do qual os dados serão restaurados: Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site . Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem . Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela

Opção	Descrição
	<p>Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.</p>
Ponto de Restauração	<p>Para operações de restauração on demand, selecione uma captura instantânea a partir da lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, especifique a instância que você gostaria de restaurar para cada origem escolhida e clique em **Avançar**:

Host ou Cluster ESX Original

Selecione esta opção para restaurar dados para o host ou cluster original.

Host ou Cluster do ESX Alternativo

Selecione esta opção para restaurar dados para um destino local que seja diferente do host ou cluster original e, em seguida, selecione o local alternativo a partir dos recursos disponíveis. As redes de teste e de produção podem ser configuradas no local alternativo para criar uma rede protegida, que evita que máquinas virtuais usadas para teste interfiram com máquinas virtuais

usadas para produção. Na seção **vCenters**, selecione um local alternativo. É possível filtrar os locais alternativos por hosts ou clusters.

No campo **Destino da pasta da MV**, insira o caminho da pasta da máquina virtual no armazenamento de dados de destino. Observe que o diretório será criado se não existir um. Use "/" como a pasta de máquina virtual raiz do armazenamento de dados direcionado.

Host ESX se vCenter estiver inativo

Selecione esta opção para efetuar bypass no vCenter e restaurar dados diretamente no host do ESX. Em outros cenários de restauração, as ações são concluídas por meio do vCenter. Se o vCenter estiver indisponível, esta opção restaurará a máquina virtual do vCenter ou máquinas virtuais das quais o vCenter depende.

5. Na página **Configurar armazenamento de dados**, execute as ações a seguir:

- Se você estiver restaurando dados em um host ou cluster do ESX alternativo, selecione o armazenamento de dados de destino e clique em **Avançar**.
- Se você estiver restaurando dados no host ou cluster do ESX original, não será necessário configurar um armazenamento de dados. Clique em **Avançar**.

6. Na página **Configurar rede**, especifique as configurações de rede a serem usadas para cada origem escolhida e clique em **Avançar**.

- Se você estiver restaurando dados no host ou cluster do ESX original, especifique as configurações de rede a seguir:

Permitir que o sistema defina a configuração de IP

Selecione esta opção para permitir que seu sistema operacional defina o endereço IP de destino. Durante uma operação de restauração de modo de teste, a máquina virtual de destino recebe um novo endereço de MAC juntamente com uma NIC associada. Dependendo de seu sistema operacional, um novo endereço IP pode ser designado com base na NIC original da máquina virtual, ou designado por meio do DHCP. Durante uma restauração do modo de produção, o endereço de Controle de Acesso à Mídia não é alterado; portanto, o endereço IP deve ser retido.

Usar configuração de IP original

Selecione essa opção para restaurar no host ou cluster original usando a configuração de endereço IP predefinida. Durante a operação de restauração, a máquina virtual de destino recebe um novo endereço de MAC, mas o endereço IP é retido.

- Se você estiver restaurando dados em um host ou cluster ESX alternativo, conclua as etapas a seguir:
 - a. Nos campos **Produção e Teste**, configure as redes virtuais para as execuções de tarefas de restauração de produção e de teste. As configurações de rede de destino para ambientes de produção e de teste devem apontar para locais diferentes para criar uma rede protegida, o que evita que as máquinas virtuais usadas para teste interfiram com as máquinas virtuais usadas para produção. As redes que estão associadas aos modos de teste e de produção serão usadas quando a tarefa de restauração for executada no modo associado.
 - b. Configure um endereço IP ou máscara de sub-rede para máquinas virtuais a serem reaproveitadas para casos de uso de desenvolvimento, teste ou recuperação de desastre. Os tipos de mapeamento suportados incluem IP para IP, IP para DHCP e sub-rede para sub-rede. Máquinas virtuais que contêm várias NICs são suportadas.

Execute uma das seguintes ações:

- Para permitir que o sistema operacional defina as sub-redes de destino e os endereços IP, clique em **Usar sub-redes e endereços IP definidos pelo sistema para o S.O. guest da MV no destino**.
- Para usar suas sub-redes e seus endereços IP predefinidos, clique em **Usar sub-redes e endereços IP originais para o S.O. guest da MV no destino**.
- Para criar uma nova configuração de mapeamento, selecione **Incluir mapeamentos para sub-redes e endereços IP para o S.O. guest da MV no destino**, clique em **Incluir**

mapeamento e insira uma sub-rede ou um endereço IP no campo **Incluir sub-rede ou endereço IP de origem**.

Escolha um dos protocolos de rede a seguir:

- Selecione **DHCP** para selecionar automaticamente um IP e informações de configuração relacionadas se o DHCP estiver disponível na origem selecionada.
- Selecione **Estático** para inserir uma sub-rede ou endereço IP, máscara de sub-rede, gateway e DNS específicos. **Sub-rede / Endereço IP, Máscara de sub-rede e Gateway** são campos obrigatórios. Se uma sub-rede for inserida como uma origem, uma sub-rede também deve ser inserida como um destino.

A reconfiguração de IP será ignorada para as máquinas virtuais se um IP estático for usado, mas nenhum mapeamento de sub-rede adequado for localizado, ou se a máquina virtual de origem estiver desligada e houver mais de uma NIC associada. Em um ambiente Windows, caso a máquina virtual use apenas DHCP, a reconfiguração de IP será ignorada para essa máquina virtual. Em um ambiente Linux, todos os endereços são considerados estáticos e apenas o mapeamento de IP ficará disponível.

7. Nos **Métodos de restauração**, selecione o método de restauração a ser usado para seleção de origem. Configure a tarefa de restauração do VMware para ser executada no modo de teste, produção ou clone por padrão. Depois que a tarefa é criada, ela pode ser executada no modo de produção ou de clonagem por meio da área de janela **Sessões da tarefa**. Também é possível mudar o nome da MV restaurada inserindo o novo nome da MV no campo **Renomear MV (opcional)**. Clique em **Avançar** para continuar.
8. Na página **Opções da tarefa (opcional)**, configure opções avançadas e clique em **Avançar**.

Tornar o recurso de clone IA permanente

Ative esta opção para mover o disco virtual para armazenamento permanente e limpar recursos temporários. Esta ação é realizada iniciando uma operação do vMotion para os recursos em segundo plano. O destino da operação do vMotion é o Armazenamento de dados de configuração da VM. O disco de Acesso Instantâneo ainda está disponível para operações de leitura/gravação durante esta operação.

Ligar após a recuperação

Altere o estado da energia de uma máquina virtual após a execução de uma recuperação. As máquinas virtuais são ligadas na ordem em que elas são recuperadas, conforme definido na etapa Origem.

Restrição: Os modelos de máquina virtual restaurados não podem ser ligados após a recuperação.

Sobrescrever máquina virtual

Ative esta opção para permitir que a tarefa de restauração sobrescreva a máquina virtual selecionada. Por padrão, essa opção está desativada.

Continuar com a restauração mesmo que ela falhe

Altere a recuperação de um recurso em uma série se a recuperação do recurso anterior falhar. Se desativada, a tarefa de restauração será parada se a recuperação de um recurso falhar.

Executar limpeza imediatamente na falha da tarefa

Ative esta opção para limpar automaticamente os recursos alocados como parte de uma tarefa de restauração, se a recuperação da máquina virtual falhar.

Permitir sobrescrever e forçar limpeza de sessões antigas pendentes

Ative esta opção para permitir que uma sessão planejada de uma tarefa de recuperação force uma sessão pendente existente a limpar recursos associados para que a nova sessão possa ser executada. Desative esta opção para manter um ambiente de teste existente em execução sem ser limpo.

Restaurar tags VM

Ative esta opção para restaurar tags que são aplicadas às máquinas virtuais por meio do vSphere.

Corrigir arquivo VMX para disco ausente

Se discos individuais forem excluídos de um backup, a máquina virtual associada falhará ao iniciar. Ative esta opção para remover as entradas para discos excluídos do arquivo de configuração do VMX e assegurar que a máquina virtual restaurada seja iniciada como parte de uma tarefa de restauração de VM instantânea.

Anexar Sufixo ao Nome da Máquina Virtual

Insira um sufixo a ser incluído nos nomes de máquinas virtuais restauradas.

Prepender prefixo para nome da máquina virtual

Insira um prefixo a ser incluído nos nomes de máquinas virtuais restauradas.

9. Opcional: Na página **Aplicar scripts**, escolha as opções de script a seguir e clique em **Avançar**.

- Selecione **Pré-script** para selecionar um script transferido por upload e um servidor de aplicativos ou de script no qual o pré-script é executado. Para selecionar um servidor de aplicativos no qual o script será executado, desmarque a caixa de seleção **Usar servidor de script**. Acesse a página **Configuração do sistema > Script** para configurar scripts e servidores de script.
- Selecione **Pós-script** para selecionar um script transferido por upload e um servidor de aplicativos ou de script no qual o pós-script é executado. Para selecionar um servidor de aplicativos no qual o script é executado, desmarque a caixa de seleção **Usar servidor de script**. Navegue para a página **Configuração do sistema > Script** para configurar scripts e servidores de script.
- Selecione **Continuar a tarefa durante erro do script** para continuar executando a tarefa quando o script que está associado à tarefa falhar. Quando esta opção estiver ativada e o pré-script for concluído com um código de retorno diferente de zero, a tarefa de backup ou de restauração continuará sendo executada e o status da tarefa de pré-script retornará COMPLETED. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa de pós-script retornará COMPLETED. Quando esta opção não estiver selecionada, a tarefa de backup ou de restauração não será executada, e o status da tarefa de pré-script ou pós-script será retornado com um status FAILED.

10. Execute uma das ações a seguir na página **Planejamento**:

- Para executar uma tarefa on demand, clique em **Avançar**.
- Para configurar uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique quando e a frequência com que a tarefa de restauração deverá ser iniciada. Clique em **Avançar**.

11. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

As tarefas on demand serão iniciadas imediatamente; as tarefas recorrentes iniciarão no horário de início planejado.

O que Fazer Depois

Após a conclusão da tarefa, selecione uma das opções a seguir, no menu **Ações**, nas seções Sessões de tarefas ou Clones ativos na área de janela **Restaurar**:

Limpeza

Destrói a máquina virtual e limpa todos os recursos associados. Como esta é uma máquina virtual temporária a ser usada para teste, todos os dados são perdidos quando a máquina virtual é destruída.

Mover para produção (vMotion)

Migra a máquina virtual por meio do vMotion para o armazenamento de dados e a Rede virtual definida como a rede de produção.

Clone (vMotion)

Migra a máquina virtual por meio do vMotion para o armazenamento de dados e a Rede virtual definida como a rede de teste.

Tarefas relacionadas

[“Incluindo uma Instância do vCenter Server” na página 95](#)

Quando uma instância do vCenter Server é incluída no IBM Spectrum Protect Plus, um inventário da instância é capturado, permitindo concluir tarefas de backup e restauração, bem como executar relatórios.

Criando uma rede protegida por meio de uma tarefa de restauração do VMware

Por meio da rede protegida, é possível estabelecer um ambiente seguro para testar suas tarefas sem interferir com as máquinas virtuais usadas para produção. A rede protegida pode ser usada com tarefas que estão em execução no modo de teste e no modo de produção.

Antes de Iniciar

Crie e execute uma tarefa de Restauração do VMware. Para obter instruções, consulte [“Restaurando Dados do VMware”](#) na página 111.

Procedimento

Para criar uma rede protegida, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > VMware**.
2. Na área de janela **Restauração**, revise os pontos de restauração disponíveis das origens do VMware, incluindo máquinas virtuais, modelos de VM, armazenamentos de dados, pastas e vApps. Use a função de procura e filtros para otimizar sua seleção em tipos de site de recuperação específicos. Expanda uma entrada na área de janela **Restaurar** para visualizar pontos de restauração individuais por data.
3. Selecione pontos de restauração e clique no ícone Incluir na lista de restauração  para incluir o ponto de restauração na Lista de restauração. Clique no ícone remover  para remover itens da Lista de restauração.
4. Clique em **Opções** para configurar as opções de definição de tarefa.
5. Selecione **Host ESX ou cluster alternativo**, em seguida, selecione um host ou cluster alternativo da lista do vCenter.
6. Expanda a seção **Configurações de Rede**. Nos campos **Produção** e **Teste**, configure redes virtuais para execuções de tarefas de Restauração de produção e de teste. As configurações de rede de destino para ambientes de produção e de teste devem ser locais diferentes para criar uma rede protegida, que evita que máquinas virtuais usadas para teste interfiram com máquinas virtuais usadas para produção. As redes associadas ao Teste e à Produção serão utilizadas quando a tarefa de restauração for executada no modo associado. Os endereços IP da máquina de destino podem ser configurados usando as seguintes opções:

Usar sub-redes e endereços IP definidos pelo sistema para S.O. guest da VM no destino

Selecione para permitir que seu sistema operacional defina o endereço IP de destino. Durante uma restauração de Modo de teste, a máquina virtual de destino recebe um novo endereço de MAC junto com uma NIC associada. Dependendo de seu sistema operacional, um novo endereço IP pode ser designado com base na NIC original da máquina virtual, ou designado por meio do DHCP. Durante uma operação de restauração de Modo de produção, o endereço de MAC não muda; portanto, o endereço IP deve ser retido.

Usar sub-redes e endereços IP originais para S.O. guest da VM no destino

Selecione para restaurar para o host ou cluster original usando sua configuração de endereço IP predefinido. Durante uma restauração, a máquina virtual de destino recebe um novo endereço de MAC, mas o endereço IP é retido.

Defina as configurações de rede para uma restauração em um host ou cluster ESX alternativo ou de longa distância:

Nos campos **Produção** e **Teste**, configure redes virtuais para execuções de tarefas de restauração de produção e teste. As configurações de rede de destino para ambientes de produção e de teste devem ser locais diferentes para criar uma rede protegida, que evita que máquinas virtuais usadas para teste interfiram com máquinas virtuais usadas para produção. As redes associadas ao Teste e à Produção serão utilizadas quando a tarefa de restauração for executada no modo associado.

Configure um endereço IP ou máscara de sub-rede para que máquinas virtuais tenham seu propósito redefinido para casos de uso de desenvolvimento/teste ou de recuperação de desastre. Os tipos de mapeamento suportados incluem IP para IP, IP para DHCP e sub-rede para sub-rede. Máquinas virtuais contendo várias NICs são suportadas.

Por padrão, a opção **Usar sub-redes definidas pelo sistema e endereços IP para o S.O. guest da VM no destino** é ativada. Para usar suas sub-redes e endereços IP predefinidos, selecione **Usar sub-redes e endereços IP originais para S.O. guest da VM no destino**.

Para criar uma nova configuração de mapeamento, selecione **Incluir mapeamentos para sub-redes e endereços IP para S.O. guest da VM no destino**, em seguida, clique em **Incluir mapeamento**. Insira uma sub-rede ou endereço IP no campo **Origem**. No campo de destino, selecione **DHCP** para selecionar automaticamente um IP e informações de configuração relacionadas se o DHCP estiver disponível no cliente selecionado. Selecione **Estático** para inserir uma sub-rede ou endereço IP, máscara de sub-rede, gateway e DNS específicos. Observe que **Sub-rede/Endereço IP, Máscara de sub-rede e Gateway** são campos obrigatórios. Se uma sub-rede for inserida como uma origem, uma sub-rede também deve ser inserida como um destino.

A reconfiguração de IP será ignorada para máquinas virtuais se for usado um IP estático, mas não for localizado nenhum mapeamento de sub-rede adequado, ou se a máquina de origem for desligada e houver mais de uma NIC associada. Em um ambiente Windows, se uma máquina virtual for somente DHCP, a reconfiguração de IP será ignorada para essa máquina virtual. Em um ambiente Linux, todos os endereços são considerados como estáticos e apenas o mapeamento de IP estará disponível.

Armazenamento de Dados de Destino

Configure o armazenamento de dados de destino para uma restauração em um host ou cluster ESX alternativo.

Destino da Pasta da VM

Insira o caminho de pasta da VM no armazenamento de dados de destino. Observe que o diretório será criado se não existir um. Use "/" como a pasta da VM raiz do armazenamento de dados direcionado.

7. Clique em **Salvar** para salvar as opções de política.
8. Após a conclusão da tarefa, selecione uma das seguintes opções do menu **Ações** nas seções Sessões de tarefas ou Clones ativos na área de janela **Restauração**:

Limpeza

Destrói a máquina virtual e limpa todos os recursos associados. Como esta é uma máquina virtual temporária/de teste, todos os dados serão perdidos quando a máquina virtual for destruída.

Mover para produção (vMotion)

Migra a máquina virtual por meio do vMotion para o Armazenamento de dados e a Rede virtual definida como a rede de "Produção".

Clone (vMotion)

Migra a máquina virtual por meio do vMotion para o Armazenamento de dados e a Rede virtual definida como a rede de "Teste".

Tarefas relacionadas

[“Incluindo uma Instância do vCenter Server”](#) na página 95

Quando uma instância do vCenter Server é incluída no IBM Spectrum Protect Plus, um inventário da instância é capturado, permitindo concluir tarefas de backup e restauração, bem como executar relatórios.

Restaurando dados quando o vCenter ou outras VMs de gerenciamento não estão acessíveis

O IBM Spectrum Protect Plus fornece uma opção para restaurar dados automaticamente usando hosts ESXi se o vCenter não estiver acessível. Essa opção restaura a máquina virtual (VM) do vCenter ou as VMs das quais o vCenter depende.

Sobre Esta Tarefa

Esse procedimento pode ser usado se qualquer um dos serviços de gerenciamento a seguir estiver parcial ou totalmente perdido em seu ambiente:

- vCenter
- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)
- Active Directory (AD)
- Servidores de Sistema de Nomes de Domínio (DNS)

Para recuperar dados sem um vCenter, o host ESXi deve ter um comutador padrão ou um comutador distribuído pré-existente com ligação efêmera. Se esses requisitos não forem atendidos, será necessário criar um novo comutador padrão no host ESXi. Se não houver uplinks disponíveis para o comutador padrão, o comutador padrão deverá ser removido do comutador distribuído.

O procedimento descreve etapas manuais adicionais que são necessárias para concluir uma operação de restauração quando a operação está em execução em um ambiente do vCenter Server (VCS).

A recuperação de uma VM de gerenciamento em um ambiente VCS pode resultar na perda de acesso à VM. A perda de acesso é devido a uma configuração incorreta do comutador virtual. Conclua as etapas a seguir na VM afetada para recuperar-se desse estado e para concluir uma operação de recuperação.

Procedimento

1. Conecte-se ao host da interface com o usuário do ESXi de destino e crie um novo comutador virtual padrão. Neste ponto, não há grupos de portas ou uplinks disponíveis para o comutador.
2. Use o protocolo SSH para conectar-se ao servidor ESXi. Identifique e selecione a NIC física e o grupo de portas do comutador virtual distribuído existente que é denominado SDDC-Dswitch-Private. O exemplo a seguir faz referência a uma Placa de Interface de Rede virtualizada (VNIC) denominada `vmnic0`, que faz parte do ID de porta 64. É possível listar as informações do comutador virtual distribuído (DVS) emitindo o comando a seguir:

```
#esxcli network vswitch dvs vmware list
```

3. Com base nas informações anteriores, remova a NIC e o ID da porta (grupo de portas) do DVS SDDC-Dswitch-Private usando o comando a seguir. Use o ID da porta da etapa 2.

```
#esxcfg-vswitch -Q physical_vnic -V port_group SDDC-Dswitch-Private
```

4. Inclua a NIC e o grupo de portas no comutador padrão que você criou na etapa 1 emitindo o comando a seguir em uma linha:

```
#esxcli network vswitch standard uplink add --uplink-name=physical_vnic --vswitch-name=standard_vswitch
```

5. Na interface do ESXi, inclua um grupo de portas e selecione o comutador virtual padrão. O comutador virtual deve ter um uplink e um grupo de portas.
6. Execute uma operação de restauração em IBM Spectrum Protect Plus com a opção **Host ESX se o vCenter estiver desativado** ativada.
7. Clique em **Opções** ao definir a operação de restauração no IBM Spectrum Protect Plus e escolha o novo comutador de rede que você criou na etapa 1 em **Rede**.
8. Usando a interface com o usuário do ESXi de destino, ligue a VM recuperada.
9. Após as VMs estarem acessíveis, efetue login na interface com o usuário do vCenter e inicie a migração das VMs de gerenciamento do grupo de portas temporário criado na etapa 5 para o grupo da porta distribuído original, SDDC-DPortGroup-Mgmt.

Inicie uma migração a partir da guia **Rede** selecionando um data center e, em seguida, clicando em **Migrar VMs para outra rede** no menu **Ações**. Selecione a rede de origem (o comutador temporário criado na etapa 5) e a rede de destino (o comutador de gerenciamento).

10. Após todas as VMs serem migradas para o grupo de portas original, reincorpore a NIC física e o grupo de porta no comutador virtual distribuído original, executando as ações a seguir:
 - a. Remova as placas de rede (conhecidas como vmnics) de um vSwitch padrão que foi redesignado anteriormente, emitindo o seguinte comando:

```
#esxcli network vswitch standard uplink remove --uplink-name=vmnic --vswitch-name=vSwitch
```

Por exemplo:

```
#esxcli network vswitch standard uplink remove --uplink-name=vmnic0
```

```
--vswitch-name=vered_recovery
```

- b. Inclua placas de rede em um Comutador Distribuído VNetwork (vDS) emitindo o comando a seguir:

```
#esxcfg-vswitch -P vmnic -V unused_dvPort_ID dvSwitch # add a vDS uplink
```

Por exemplo:

```
#esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
```

11. Exclua o grupo de portas temporário e o vSwitch padrão da interface com o usuário do host ESXi.
12. Depois que as VMs estiverem migradas e acessíveis, use a interface com o usuário do host ESXi para cancelar, mas não excluir, o registro das VMs antigas se o host original estiver acessível. Ao usar esse método, você evita a criação de informações duplicadas, como nomes, endereços de Controle de Acesso à Mídia (MAC), IDs de nível do sistema operacional e identificadores exclusivos universais (UUIDs) da VM. Deve-se concluir essa etapa mesmo se estiver usando um novo armazenamento de dados.

Em algumas versões do vSphere ou ESXi, a operação de remoção de registro pode ser concluída usando a opção **Remover do inventário**. Isso cancela o registro de uma VM no catálogo do vCenter, mas deixa os arquivos VMDK, que consomem espaço de armazenamento, no armazenamento de dados. Após ter recuperado totalmente a VM e o ambiente estar executando com êxito, é possível recuperar o espaço removendo manualmente esses arquivos do armazenamento de dados.

Fazendo Backup e Restaurando Dados do Hyper-V

Para proteger dados do Hyper-V, primeiro inclua servidores Hyper-V no IBM Spectrum Protect Plus e, em seguida, crie tarefas para operações de backup e restauração para o conteúdo dos servidores.

Certifique-se de que o ambiente Hyper-V atenda aos requisitos do sistema em [“Requisitos do Hypervisor”](#) na página 23.

Incluindo um servidor Hyper-V

Quando um servidor Hyper-V é incluído no IBM Spectrum Protect Plus, é capturado um inventário do servidor, que permite concluir tarefas de backup e restauração, além de executar relatórios.

Antes de Iniciar

Observe as seguintes considerações e procedimentos antes de incluir um servidor Hyper-V no IBM Spectrum Protect Plus:

- Os servidores Hyper-V podem ser registrados usando um nome de DNS ou endereço IP. Os nomes de DNS devem ser resolvidos por IBM Spectrum Protect Plus. Se o servidor Hyper-V for parte de um cluster, todos os nós no cluster deverão ser resolvíveis por meio de DNS. Se o DNS não estiver disponível, o servidor deverá ser incluído no arquivo `/etc/hosts` no dispositivo IBM Spectrum Protect Plus. Se mais de um servidor Hyper-V estiver configurado em um ambiente em cluster, todos os

servidores deverão ser incluídos em /etc/hosts. Ao registrar o cluster no IBM Spectrum Protect Plus, registre o Gerenciador de Cluster de Failover.

- Todos os servidores Hyper-V, incluindo nós do cluster, devem ter o Serviço do inicializador iSCSI da Microsoft em execução em sua lista de Serviços. Configure o serviço como Automático para que ele esteja disponível quando a máquina inicializar.
- Inclua o usuário no grupo de administradores locais no servidor Hyper-V.

Procedimento

Para incluir um servidor Hyper-V, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > Hyper-V**.
2. Clique em **Gerenciar o Hyper-V Server**.
3. Clique em **Incluir servidor Hyper-V**.
4. Preencha os campos na área de janela **Propriedades do servidor**:

Hostname/IP

Insira o endereço IP resolvível ou um caminho e nome de máquina resolvíveis.

Usar usuário existente

Ative para selecionar um nome de usuário e senha inseridos anteriormente para o servidor.

Nome de Usuário

Insira seu nome de usuário para o servidor.

Password

Insira sua senha para o servidor.

Porta

Insira a porta de comunicações do servidor que está sendo incluído. A porta padrão típica é 5985.

Selecione a caixa de seleção **Usar SSL** para ativar uma conexão Secure Sockets Layer (SSL) criptografada.

Para ativar uma conexão SLL, deve-se incluir o certificado SSL autoassinado para o servidor Hyper-V ou um certificado de autoridade de certificação (CA). Para fazer upload de um certificado, consulte [“Fazendo upload de um certificado SSL a partir do console administrativo”](#) na página 280.

Se você não selecionar **Usar SSL**, deverá concluir etapas adicionais no servidor Hyper-V. Consulte [“Ativando o WinRM para conexão com servidores Hyper-V”](#) na página 123.

5. Na seção **Opções**, configure a seguinte opção:

Número máximo de VMs a serem processadas simultaneamente por servidor Hyper-V

Configure o número máximo de capturas instantâneas de máquina virtual simultâneas para processamento no servidor Hyper-V.

6. Clique em **Salvar**. O IBM Spectrum Protect Plus confirma uma conexão de rede, inclui o servidor no banco de dados e, em seguida, cataloga o servidor.

Se aparecer uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se suas entradas estiverem corretas e a conexão for malsucedida, entre em contato com um administrador do sistema para revisar as conexões.

O que Fazer Depois

Depois de incluir o servidor Hyper-V, conclua a seguinte ação:

Ação	Como
Designar permissões de usuário para o hypervisor.	Consulte “Criando uma função” na página 302.

Tarefas relacionadas

[“Fazendo Backup de Dados do Hyper-V”](#) na página 124

Use uma tarefa de backup para fazer backup de dados do Hyper-V com capturas instantâneas.

[“Restaurando dados do Hyper-V”](#) na página 127

As tarefas de restauração do Hyper-V suportam cenários de Restauração da VM instantânea e de Restauração de disco instantâneo, que são criados automaticamente com base na origem selecionada.

Ativando o WinRM para conexão com servidores Hyper-V

Se não for possível usar SSL para ativar o tráfego de rede criptografado entre servidores Hyper-V do IBM Spectrum Protect Plus, o WinRM deve ser configurado no host para permitir o tráfego de rede não criptografado. Certifique-se de que tenha entendido os riscos de segurança que estão associados com a permissão do tráfego de rede não criptografado.

Procedimento

Para configurar o WinRM para conexão com hosts Hyper-V:

1. No sistema host Hyper-V, efetue login com uma conta do administrador.
2. Abra um prompt de comandos do Windows. Se o Controle de Conta do Usuário (UAC) estiver ativado, você deverá abrir o prompt de comandos com privilégios elevados, executando com a opção "Executar como administrador" ativada.
3. Insira o seguinte comando para configurar o WinRM para permitir o tráfego de rede não criptografado:

```
winrm s winrm/config/service @{AllowUnencrypted="true"}
```

4. Verifique se a opção AllowUnencrypted está configurada como true por meio do seguinte comando:

```
winrm g winrm/config/service
```

Detectando recursos do Hyper-V

Os recursos do Hyper-V são detectados automaticamente após a inclusão do servidor Hyper-V no IBM Spectrum Protect Plus. No entanto, é possível executar uma tarefa de inventário para detectar quaisquer mudanças que ocorreram desde que o servidor foi incluído.

Procedimento

Para executar uma tarefa de inventário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > Hyper-V**.
2. Na lista de servidores Hyper-V, selecione um servidor ou clique no link para o servidor para navegar para o recurso desejado. Por exemplo, se desejar executar uma tarefa de inventário para uma máquina virtual individual em um servidor, clique no link do servidor e, em seguida, selecione uma máquina virtual.
3. Clique em **Executar Inventário**.

Testando a conexão com uma máquina virtual Hyper-V Server

É possível testar a conexão com a máquina virtual Hyper-V Server. A função de teste verifica a comunicação com a máquina virtual e testa as configurações de DNS entre o dispositivo virtual IBM Spectrum Protect e a máquina virtual.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > Hyper-V**.
2. Na lista de Servidores Hyper-V, clique no link para uma máquina virtual do Hyper-V Server para navegar para as máquinas virtuais individuais.
3. Selecione uma máquina virtual e, em seguida, clique em **Selecionar opções**.
4. Selecione **Usar usuário existente**.
5. Selecione um usuário na lista **Selecionar usuário**.
6. Clique em **Testar**.

Fazendo Backup de Dados do Hyper-V

Use uma tarefa de backup para fazer backup de dados do Hyper-V com capturas instantâneas.

Antes de Iniciar

Observe os seguintes procedimentos e considerações antes de criar uma definição de tarefa de backup:

- Registre os provedores dos quais você deseja fazer backup. Para obter mais informações, consulte [“Incluindo um servidor Hyper-V”](#) na página 121
- Configure políticas do SLA. Para obter instruções, consulte [“Criar políticas de backup”](#) na página 73.
- As tarefas de Backup e restauração do Hyper-V requerem a instalação dos serviços de integração mais recentes do Hyper-V.

Para ambientes Microsoft Windows, consulte [Sistemas operacionais guest Windows para Hyper-V suportados no Windows Server](#).

Para ambientes Linux, consulte [Máquinas virtuais Linux e FreeBSD suportadas para Hyper-V no Windows](#).

- Todos os servidores Hyper-V, incluindo nós do cluster, devem ter o Serviço do inicializador iSCSI da Microsoft em execução em sua lista de Serviços. Configure o serviço como Automático para que ele esteja disponível quando a máquina inicializar.
- Antes de um usuário do IBM Spectrum Protect Plus poder concluir operações de backup e restauração, as funções devem ser designadas ao usuário. Conceda aos usuários acesso a hypervisors e a operações de backup e restauração por meio da área de janela **Contas**. As funções e permissões associadas são designadas durante a criação da conta do usuário. Para obter mais informações, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297 e [“Gerenciando contas do usuário”](#) na página 305.
- Se uma máquina virtual estiver associada a várias políticas de ANS, certifique-se de que as políticas não estejam planejadas para execução simultaneamente. Planeje as políticas de ANS para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de ANS.
- Se o endereço IP do dispositivo IBM Spectrum Protect Plus mudar após a criação de um backup de base inicial do Hyper-V, o IQN de destino do recurso do Hyper-V poderá ficar em um estado inválido. Para corrigir esse problema, a partir da ferramenta Inicializador iSCSI da Microsoft, clique na guia **Descoberta**. Selecione o endereço IP antigo, em seguida, clique em **Remover**. Clique na guia **Destino** e desconecte a sessão de reconexão.
- Se uma VM for protegida por uma política de ANS, os backups da VM serão retidos com base nos parâmetros de retenção da política de ANS, mesmo se a VM for removida.

Procedimento

Para definir uma tarefa de backup do Hyper-V, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > Hyper-V**.

2. Selecione os recursos para fazer backup.

Use a função de procura para procurar os recursos disponíveis e comutar os recursos exibidos por meio do filtro **Visualização**. As opções disponíveis são **VMs** e **Armazenamento de dados**.

3. Clique em **Selecionar política de ANS** para incluir uma ou mais políticas de ANS que atendem aos critérios de dados de backup para a definição de tarefa.

4. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.

A tarefa é executada conforme definido pelas políticas de SLA selecionadas. Para executar a tarefa manualmente, clique em **Tarefas e operações > Planejamento**. Selecione a tarefa e clique em **Ações > Iniciar**.

Dica: o botão **Executar** é ativado somente para um backup de hypervisor único e o hypervisor deve ter uma política de ANS aplicada.

5. Para editar opções antes de iniciar a tarefa, clique no ícone editar na tabela **Selecionar opções**.

Na seção **Opções de backup**, configure as seguintes opções de definição de tarefa:

Ignorar armazenamentos de dados somente leitura

Ative para ignorar armazenamentos de dados montados como somente leitura.

Ignorar armazenamentos de dados temporários montados para acesso instantâneo

Ative para excluir armazenamentos de dados de Acesso instantâneo temporários da definição de tarefa de backup.

Prioridade

Configure a prioridade de backup do recurso selecionado. Os recursos com uma configuração de prioridade mais alta são submetidos a backup primeiro na tarefa. Clique no recurso que você deseja priorizar na seção **Backup do VMware** e, em seguida, configure a prioridade de backup no campo **Prioridade**. Configure 1 para o recurso de prioridade mais alta ou 10 para a mais baixa. Quando um valor de prioridade não é configurado, a opção designa automaticamente uma prioridade de 5 é configurada por padrão.

Na seção **Opções de captura instantânea**, configure as seguintes opções de definição de tarefa:

Tornar o aplicativo de captura instantânea da VM / sistema de arquivos consistente

Ative esta opção para ativar a consistência do aplicativo ou do sistema de arquivos para a captura instantânea de máquina virtual.

Tentativas de nova tentativa de captura instantânea da VM

Configure o número de vezes que o IBM Spectrum Protect Plus deve tentar obter a captura instantânea de uma máquina virtual antes de cancelar a tarefa.

Na seção **Opções do agente**, configure as seguintes opções de definição de tarefa:

Truncate os logs SQL

Para truncar logs do aplicativo para SQL durante a tarefa de backup, ative a opção **Truncar logs SQL**. Observe que as credenciais devem ser estabelecidas para a máquina virtual associada por meio das opções Nome de usuário de S.O. `guest` e Senha de S.O. `guest` na definição de tarefa de backup. A identidade do usuário segue o formato padrão `domain\name` se a máquina virtual for conectada a um domínio. O formato `local_administrator` será usado se o usuário for um administrador local.

A identidade do usuário deve ter privilégios de administrador local. Além disso, no SQL server, a credencial de login do sistema deve ter permissões SQL `sysadmin` ativadas, bem como o direito **Efetuar logon como um serviço**. Para obter informações adicionais sobre este direito, consulte [Incluir o direito Efetuar logon como um serviço em uma conta](#).

O IBM Spectrum Protect Plus gera logs pertencentes à função de truncamento do log e copia-os para o seguinte local no dispositivo IBM Spectrum Protect Plus:

```
/data/log/guestdeployer/ latest_date / latest_entry / vm_name
```

Em que `latest_date` é a data em que ocorreu o truncamento da tarefa de backup e do log, `latest_entry` é o identificador exclusivo universal (UUID) para a tarefa e `vm_name` é o nome do host ou endereço IP da VM na qual ocorreu o truncamento do log.

Restrição: A indexação de arquivo e a restauração de arquivo não são suportadas a partir de pontos de restauração que foram transferidos para um servidor IBM Spectrum Protect.

Metadados do Arquivo de Catálogo

Para ativar a indexação de arquivo para a captura instantânea associada, ative a opção Metadados do arquivo de catálogo. Após a conclusão da indexação de arquivo, os arquivos individuais podem ser restaurados usando a área de janela **Restauração de arquivo** no IBM Spectrum Protect Plus. Observe que as credenciais devem ser estabelecidas para a máquina virtual associada usando uma chave SSH ou as opções Nome de usuário de S.O. `guest` e Senha de S.O. `guest` na definição de tarefa de backup. Certifique-se de que a máquina virtual possa ser acessada a partir do dispositivo IBM Spectrum Protect Plus usando DNS ou nome do host. Observe que as chaves SSH não são um mecanismo de autorização válido para plataformas Windows.

Arquivos de Exclusão

Insira diretórios a serem ignorados quando a indexação de arquivo for executada. Os arquivos nesses diretórios não são incluídos no catálogo do IBM Spectrum Protect Plus e não estão disponíveis para recuperação de arquivo. Os diretórios podem ser excluídos por meio de uma correspondência exata ou com asteriscos curinga especificados antes do padrão (*test) ou depois do padrão (test*). Vários curingas asteriscos também são suportados em um único padrão. Os padrões suportam caracteres alfanuméricos padrão, bem como os seguintes caracteres especiais: - _ e *. Separe vários filtros com um ponto-e-vírgula.

Utilizar usuário existente

Ative para selecionar um nome do usuário e senha inseridos anteriormente para o provedor.

Guest OS Username / Password

Para algumas tarefas (como catalogar metadados do arquivo, restauração de arquivo e reconfiguração de IP), as credenciais devem ser estabelecidas para a máquina virtual associada. Insira o nome do usuário e a senha e certifique-se de que a máquina virtual possa ser acessada a partir do dispositivo IBM Spectrum Protect Plus, por meio do DNS ou do nome do host.

A política de segurança padrão usa o protocolo Windows NTLM e a identidade do usuário segue o formato padrão *domain\name* se a máquina virtual Hyper-V estiver conectada a um domínio. O formato *local_administrator* será usado se o usuário for um administrador local.

6. Para resolver problemas de uma conexão com uma máquina virtual do hypervisor, use a função **Testar**.

A função **Testar** verifica a comunicação com a máquina virtual e testa configurações de DNS entre o dispositivo IBM Spectrum Protect Plus e a máquina virtual. Para testar uma conexão, selecione uma única máquina virtual, em seguida, clique em **Selecionar opções**. Selecione **Usar usuário existente** e selecione um nome de usuário e senha inseridos anteriormente para o recurso. O botão **Testar** é exibido à direita do botão **Salvar** na seção **Opções**. Clique em **Testar**.

7. Clique em **Salvar**.

8. Para configurar opções adicionais, clique no campo **Opções de política** que está associado à tarefa na seção **Status de política de ANS**. Configure as opções de política adicionais:

Pré-scripts e Pós-scripts

Execute um pré-script ou um post-script. Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de uma tarefa no nível de tarefa. As máquinas baseadas no Windows suportam scripts em Lote e PowerShell enquanto as máquinas baseadas no Linux suportam shell scripts.

Na seção **Pré-script** ou **Pós-script**, selecione um script transferido por upload e um servidor de script no qual o script será executado. Os scripts e servidores de script são configurados na página **Configuração do sistema > Script**.

Para continuar executando a tarefa se o script associado à tarefa falhar, selecione **Continuar a tarefa durante erro do script**.

Quando esta opção é ativada, se um pré-script ou pós-script concluir o processamento com um código de retorno diferente de zero, será feita uma tentativa de operação de backup ou de restauração e o status da tarefa de pré-script será relatado como CONCLUÍDO. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa de pós-script será relatado como CONCLUÍDO.

Quando esta opção é desativada, não é feita tentativa de backup ou de restauração e o status da tarefa de pré-script ou pós-script é relatado como COM FALHA.

Executar inventário antes do backup

Execute uma tarefa de inventário e capture os dados mais recentes dos recursos selecionados antes de iniciar a tarefa de backup.

Recursos de Exclusão

Exclua recursos específicos da tarefa de backup por meio de um único padrão ou de vários padrões de exclusão. Os recursos podem ser excluídos por meio de uma correspondência exata ou com asteriscos curinga especificados antes do padrão (*test) ou depois do padrão (test*).

Vários curingas asteriscos também são suportados em um único padrão. Os padrões suportam caracteres alfanuméricos padrão, bem como os seguintes caracteres especiais: - _ e *.

Separe vários filtros com um ponto-e-vírgula.

Forçar Backup Completo de Recursos

Forçar operações de backup de base para máquinas virtuais ou bancos de dados específicos na definição da tarefa de backup. Separe vários recursos com um ponto-e-vírgula.

9. Para salvar as opções adicionais configuradas, clique em **Salvar**.

O que Fazer Depois

Depois de definir uma tarefa de backup, conclua a seguinte ação:

Ação	Como
Crie uma definição de tarefa de restauração do Hyper-V.	Consulte “Restaurando dados do Hyper-V” na página 127.

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração”](#) na página 255

Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de tarefas de backup e restauração no nível de tarefa. Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts são criados localmente, transferidos por upload para seu ambiente por meio da página **Script** e, em seguida, aplicados a definições de tarefa.

Tarefas relacionadas

[“Iniciando Tarefas”](#) na página 252

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Restaurando dados do Hyper-V

As tarefas de restauração do Hyper-V suportam cenários de Restauração da VM instantânea e de Restauração de disco instantâneo, que são criados automaticamente com base na origem selecionada.

Antes de Iniciar

Execute as seguintes tarefas:

- Certifique-se de que uma tarefa de backup do Hyper-V tenha sido executada pelo menos uma vez. Para obter instruções, consulte [“Fazendo Backup de Dados do Hyper-V”](#) na página 124.
- Certifique-se de que o destino que você planeja usar para a tarefa de restauração esteja registrado no IBM Spectrum Protect Plus. Esse requisito se aplica às tarefas de restauração que restauram dados para hosts ou clusters originais.
- Assegure-se de que os serviços de integração mais recentes do Hyper-V estejam instalados.

Para ambientes MicrosoftWindows, consulte [Sistemas operacionais guest Windows para Hyper-V suportados no Windows Server](#).

Para ambientes Linux, consulte [Máquinas virtuais Linux e FreeBSD suportadas para Hyper-V no Windows](#).

- Assegure-se de que as funções apropriadas para as operações de restauração tenham sido designadas aos usuários afetados. Conceda aos usuários acesso aos hypervisors e às operações de backup e restauração na área de janela **Contas**. As funções e permissões associadas são designadas durante a criação da conta do usuário. Para obter instruções, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#) e [“Gerenciando contas do usuário”](#) na página 305.
- A indexação de arquivo e a restauração de arquivo do Windows em volumes que residem em discos dinâmicos não são suportadas.

- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Sobre Esta Tarefa

Se um Disco Rígido Virtual (VHDX) for selecionado para uma tarefa de restauração, o IBM Spectrum Protect Plus apresentará automaticamente opções para uma tarefa Restauração Instantânea de Disco, que fornece acesso gravável e instantâneo a pontos de restauração de dados e de aplicativo.

Uma captura instantânea do IBM Spectrum Protect Plus é mapeada para um servidor de destino no qual a captura instantânea pode ser acessada ou copiada conforme necessário. Todas as outras origens são restauradas utilizando tarefas de restauração da VM Instantânea, que podem ser executadas nos seguintes modos:

Modo de teste

O modo de teste cria máquinas virtuais temporárias para desenvolvimento, teste, verificação de captura instantânea e verificação de recuperação de desastre em uma base planejada e repetida sem afetar os ambientes de produção. As máquinas de teste são mantidas em execução enquanto elas são necessárias para concluir o teste e a verificação e, em seguida, são limpas. Por meio da rede protegida, é possível estabelecer um ambiente seguro para testar suas tarefas sem interferir com as máquinas virtuais usadas para produção. As máquinas virtuais que são criadas no modo de teste também recebem nomes e identificadores exclusivos para evitar conflitos dentro de seu ambiente de produção.

Modo Clone

O modo Clone cria cópias de máquinas virtuais para casos de uso que requerem cópias permanentes ou de longa execução para mineração de dados ou duplicação de um ambiente de teste em uma rede protegida. As máquinas virtuais que são criadas no modo de clonagem também recebem nomes e identificadores exclusivos para evitar conflitos dentro de seu ambiente de produção. Com o modo clone, deve-se ficar atento ao consumo de recursos, pois esse modo cria máquinas virtuais permanentes ou de longo prazo.

Modo de produção

O modo de produção permite uma recuperação de desastre no site local, a partir do armazenamento primário ou em um site de recuperação de desastre remoto, substituindo imagens de máquina originais por imagens de recuperação. Todas as configurações são transportadas como parte da recuperação, incluindo nomes e identificadores, e todas as tarefas de dados de cópia que estão associadas à máquina virtual continuam em execução.

Restrição: A movimentação do modo de teste para o modo de produção não é suportada para o Hyper-V.

Procedimento

Para definir uma tarefa de restauração do Hyper-V, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Hypervisors > Hyper-V > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Hyper-V**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, execute as ações a seguir:
 - a) Revise as origens disponíveis, incluindo máquinas virtuais (MVs) e discos virtuais (VDisks). É possível expandir uma origem clicando em seu nome.

Também é possível inserir todo ou parte de um nome na caixa **Procurar** para localizar as MVs que correspondem aos critérios de procura. É possível utilizar o caractere curinga (*) para representar todo ou parte de um nome. Por exemplo, vm2* representa todos os recursos que começam com "vm2".

- b) Clique no ícone de mais  ao lado do item que você deseja incluir na lista de restauração ao lado da lista de origens. É possível incluir mais de um item do mesmo tipo (MV ou disco virtual).

Para remover um item da lista de restauração, clique no ícone de menos  ao lado do item.

- c) Clique em **Avançar**.
3. Na página **Captura instantânea de origem**, especifique a instância da MV ou do disco virtual que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar. Alguns campos não são exibidos até que um campo relacionado seja selecionado.

Opção	Descrição
Tipo de Restauração	<p>Selecione o tipo de tarefa de restauração:</p> <p>On Demand Executa uma operação de restauração única.</p> <p>Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.</p>
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual os dados serão restaurados:</p> <p>Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p>

Opção	Descrição
	Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização .
Seletor de Data	Para operações de restauração on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Ponto de Restauração	Para operações de restauração on demand, selecione uma captura instantânea a partir da lista de capturas instantâneas disponíveis no intervalo de dados selecionado.
Usar servidor vSnap alternativo para a tarefa de restauração	Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo . Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

4. Na página **Configurar destino**, escolha a instância a ser restaurada para a origem selecionada e clique em **Avançar**:

Host ou Cluster do Hyper-V Original

Selecione esta opção para restaurar dados para o host ou cluster original.

Host ou Cluster Alternativo do Hyper-V

Selecione esta opção para restaurar dados para um destino local que seja diferente do host ou cluster original e, em seguida, selecione o local alternativo a partir dos recursos disponíveis.

No campo **Destino da pasta da MV**, insira o caminho da pasta da máquina virtual no armazenamento de dados de destino. Observe que o diretório será criado se não existir um. Use "/" como a pasta de máquina virtual raiz do armazenamento de dados direcionado.

5. Na página **Configurar armazenamento de dados**, execute as ações a seguir:

- Se você estiver restaurando dados em um host ou cluster do Hyper-V alternativo, selecione o armazenamento de dados de destino e clique em **Avançar**.
- Se você estiver restaurando dados no host ou cluster do ESX original, não será necessário configurar um armazenamento de dados. Apenas clique em **Avançar**.

6. Na página **Configurar rede**, especifique as configurações de rede a serem usadas para cada origem escolhida e clique em **Avançar**.

- Se você estiver restaurando dados no host ou cluster do Hyper-V original, especifique as configurações de rede a seguir:

Permitir que o sistema defina a configuração de IP

Selecione esta opção para permitir que seu sistema operacional defina o endereço IP de destino. Durante uma operação de restauração de modo de teste, a máquina virtual de destino recebe um novo endereço de MAC juntamente com uma NIC associada. Dependendo de seu sistema operacional, um novo endereço IP pode ser designado com base na NIC original da máquina virtual, ou designado por meio do DHCP. Durante a restauração de modo de produção, o endereço de MAC não muda; portanto, o endereço IP deve ser retido.

Usar configuração de IP original

Selecione essa opção para restaurar no host ou cluster original usando a configuração de endereço IP predefinida. Durante a operação de restauração, a máquina virtual de destino recebe um novo endereço de MAC, mas o endereço IP é retido.

- Se você estiver restaurando dados em um host ou cluster Hyper-V alternativo, conclua as etapas a seguir:
 - a. Nos campos **Produção e Teste**, configure as redes virtuais para as execuções de tarefas de restauração de produção e de teste. As configurações de rede de destino para ambientes de produção e de teste devem apontar para locais diferentes para criar uma rede protegida, o que evita que as máquinas virtuais usadas para teste interfiram com as máquinas virtuais usadas para produção. As redes que estão associadas aos modos de teste e de produção serão usadas quando a tarefa de restauração for executada no modo associado.
 - b. Configure um endereço IP ou máscara de sub-rede para máquinas virtuais a serem reaproveitadas para casos de uso de desenvolvimento, teste ou recuperação de desastre. Os tipos de mapeamento suportados incluem IP para IP, IP para DHCP e sub-rede para sub-rede. Máquinas virtuais que contêm várias NICs são suportadas.

Execute uma das seguintes ações:

- Para permitir que o sistema operacional defina as sub-redes de destino e os endereços IP, clique em **Usar sub-redes e endereços IP definidos pelo sistema para o S.O. guest da MV no destino**.
- Para usar suas sub-redes e seus endereços IP predefinidos, clique em **Usar sub-redes e endereços IP originais para o S.O. guest da MV no destino**.
- Para criar uma nova configuração de mapeamento, selecione **Incluir mapeamentos para sub-redes e endereços IP para o S.O. guest da MV no destino**, clique em **Incluir mapeamento** e insira uma sub-rede ou um endereço IP no campo **Incluir sub-rede ou endereço IP de origem**.

Escolha um dos protocolos de rede a seguir:

- Selecione **DHCP** para selecionar automaticamente um IP e informações de configuração relacionadas se o DHCP estiver disponível na origem selecionada.
- Selecione **Estático** para inserir uma sub-rede ou endereço IP, máscara de sub-rede, gateway e DNS específicos. **Sub-rede / Endereço IP, Máscara de sub-rede e Gateway** são campos obrigatórios. Se uma sub-rede for inserida como uma origem, uma sub-rede também deve ser inserida como um destino.

A reconfiguração de IP será ignorada para as máquinas virtuais se um IP estático for usado, mas nenhum mapeamento de sub-rede adequado for localizado, ou se a máquina virtual de origem estiver desligada e houver mais de uma NIC associada. Em um ambiente Windows, caso a máquina virtual use apenas DHCP, a reconfiguração de IP será ignorada para essa máquina virtual. Em um ambiente Linux, todos os endereços são considerados estáticos e apenas o mapeamento de IP ficará disponível.

7. Nos **Métodos de restauração**, selecione o método de restauração a ser usado para as seleções de origem. Configure a tarefa de restauração do Hyper-V para ser executada no modo de teste, produção ou clone por padrão. Depois que a tarefa é criada, é possível executar a tarefa no modo de produção ou de clonagem usando a área de janela **Sessões da tarefa**. Também é possível mudar o nome da MV restaurada inserindo o novo nome da MV no campo **Renomear MV (opcional)**. Clique em **Avançar** para continuar.
8. Opcional: Na página **Opções da tarefa (opcional)**, configure opções avançadas e clique em **Avançar**.

Tornar o recurso clone IA permanente

Ative esta opção para mover o disco virtual para armazenamento permanente e limpar recursos temporários. Esta ação é realizada iniciando uma operação do vMotion para os recursos em segundo plano. O destino da operação do vMotion é o Armazenamento de dados de configuração da VM. O disco de Acesso Instantâneo ainda está disponível para operações de leitura/gravação durante esta operação.

Inicialização após a recuperação

Alternar o estado de energia de uma máquina virtual após a execução de uma recuperação. As máquinas virtuais são ligadas na ordem em que elas são recuperadas, conforme definido na etapa Origem.

Restrição: Os modelos de máquina virtual restaurados não podem ser ligados após a recuperação.

Sobrescrever máquina virtual

Ative esta opção para permitir que a tarefa de restauração sobrescreva a máquina virtual selecionada. Por padrão, essa opção está desativada.

Continuar com a restauração mesmo que ela falhe

Altere a recuperação de um recurso em uma série se a recuperação do recurso anterior falhar. Se desativada, a tarefa de restauração será parada se a recuperação de um recurso falhar.

Executar limpeza imediatamente na falha da tarefa

Ative esta opção para limpar automaticamente os recursos alocados como parte de uma tarefa de restauração, se a recuperação da máquina virtual falhar.

Permitir sobrescrever e forçar limpeza de sessões antigas pendentes

Ative esta opção para permitir que uma sessão planejada de uma tarefa de recuperação force uma sessão pendente existente a limpar recursos associados para que a nova sessão possa ser executada. Desative esta opção para manter um ambiente de teste existente em execução sem ser limpo.

Anexar Sufixo ao Nome da Máquina Virtual

Insira um sufixo a ser incluído nos nomes de máquinas virtuais restauradas.

Prepender prefixo para nome da máquina virtual

Insira um prefixo a ser incluído nos nomes de máquinas virtuais restauradas. Clique em Salvar para salvar as opções de política.

9. Opcional: Na página **Aplicar scripts**, escolha as opções de script a seguir e clique em **Avançar**.

- Selecione **Pré-script** para selecionar um script transferido por upload e um servidor de aplicativos ou de script no qual o pré-script é executado. Para selecionar um servidor de aplicativos no qual o script será executado, desmarque a caixa de seleção **Usar servidor de script**. Acesse a página **Configuração do sistema > Script** para configurar scripts e servidores de script.
- Selecione **Pós-script** para selecionar um script transferido por upload e um servidor de aplicativos ou de script no qual o pós-script é executado. Para selecionar um servidor de aplicativos no qual o script é executado, desmarque a caixa de seleção **Usar servidor de script**. Navegue para a página **Configuração do sistema > Script** para configurar scripts e servidores de script.
- Selecione **Continuar a tarefa durante erro do script** para continuar executando a tarefa quando o script que está associado à tarefa falhar. Quando esta opção estiver ativada e o pré-script for concluído com um código de retorno diferente de zero, a tarefa de backup ou de restauração continuará sendo executada e o status da tarefa de pré-script retornará COMPLETED. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa de pós-script retornará COMPLETED. Quando esta opção não estiver selecionada, a tarefa de backup ou de restauração não será executada, e o status da tarefa de pré-script ou pós-script será retornado com um status FAILED.

10. Execute uma das ações a seguir na página **Planejamento**:

- Para executar uma tarefa on demand, clique em **Avançar**.
- Para configurar uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique quando e a frequência com que a tarefa de restauração deverá ser iniciada. Clique em **Avançar**.

11. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

As tarefas on demand serão iniciadas imediatamente; as tarefas recorrentes iniciarão no horário de início planejado.

O que Fazer Depois

Após a conclusão da tarefa, selecione uma das opções a seguir, no menu **Ações**, nas seções **Sessões de tarefas** ou **Clones ativos** na área de janela **Restaurar**:

Limpeza

Destrói a máquina virtual e limpa todos os recursos associados. Como esta é uma máquina virtual temporária a ser usada para teste, todos os dados são perdidos quando a máquina virtual é destruída.

Clonar (migrar)

Migra a máquina virtual para o armazenamento de dados e a rede virtual que são definidos como a rede de teste.

Tarefas relacionadas

[“Fazendo Backup de Dados do Hyper-V”](#) na página 124

Use uma tarefa de backup para fazer backup de dados do Hyper-V com capturas instantâneas.

[“Incluindo um servidor Hyper-V”](#) na página 121

Quando um servidor Hyper-V é incluído no IBM Spectrum Protect Plus, é capturado um inventário do servidor, que permite concluir tarefas de backup e restauração, além de executar relatórios.

Restaurando arquivos

Recupere arquivos de capturas instantâneas que são criadas por tarefas de backup do IBM Spectrum Protect Plus. Os arquivos podem ser restaurados para seu local original ou um local alternativo.

Antes de Iniciar

Observe os seguintes procedimentos e considerações antes de restaurar um arquivo:

- Revise os requisitos de indexação e restauração de arquivos em [“Requisitos de Indexação de Arquivo e Restauração”](#) na página 24.
- Execute uma tarefa de backup com os metadados do arquivo de catálogo ativados. Siga estas diretrizes:
 - Certifique-se de que as credenciais sejam estabelecidas para a máquina virtual associada, e também para o destino da máquina virtual alternativa por meio das opções Nome do usuário de S.O. guest e Senha de S.O. guest na definição de tarefa de backup.
 - Certifique-se de que a máquina virtual possa ser acessada a partir do dispositivo IBM Spectrum Protect Plus por meio do DNS ou do nome do host. Em um ambiente Windows, a política de segurança padrão usa o protocolo Windows NTLM e a identidade do usuário segue o formato padrão *domain\name* se a máquina virtual Hyper-V estiver conectada a um domínio. O formato *local_administrator* será usado se o usuário for um administrador local.
 - Para que uma restauração de arquivo seja concluída com sucesso, certifique-se de que o ID do usuário que está na máquina de destino tenha as permissões de propriedade necessárias para o arquivo que está sendo restaurado. Se um arquivo foi criado por um usuário que difere do ID do usuário que está restaurando o arquivo com base nas credenciais de segurança do Windows, a tarefa de restauração de arquivo falhará.

Sobre Esta Tarefa

Restrições:

- Os sistemas de arquivos criptografados do Windows não são suportados para catalogação de arquivos ou restauração de arquivos.
- A indexação de arquivo e a restauração de arquivo não são suportadas a partir de pontos de restauração que foram transferidos para recursos em nuvem ou servidores do repositório.
- Ao restaurar arquivos em um ambiente Resilient File System (ReFS), as restaurações de versões mais recentes do Windows Server para versões anteriores não são suportadas. Por exemplo, a restauração de um arquivo do Windows Server 2016 para o Windows Server 2012.
- As restaurações de catalogação de arquivos, de backup, point-in-time e outras operações que chamam o agente do Windows falharão se um administrador local não padrão for inserido como o **Nome do usuário de S.O. guest** ao definir uma tarefa de backup. Um administrador local não padrão é qualquer usuário que foi criado no S.O. guest e recebeu a função de administrador.

Isso ocorrerá se a chave de registro `LocalAccountTokenFilterPolicy` em `[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` estiver configurada como 0 ou não configurada. Se o parâmetro estiver configurado como 0 ou não estiver configurado, um administrador local não padrão não poderá interagir com o WinRM, que é o protocolo que o IBM Spectrum Protect Plus usa para instalar o agente do Windows para catalogação de arquivos, enviar comandos para esse agente e obter resultados dele.

Configure a chave de registro `LocalAccountTokenFilterPolicy` como 1 no guest Windows que está sendo submetido a backup com Metadados do arquivo de catálogo ativados. Se a chave não existir, navegue para `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` e inclua uma chave de Registro DWORD chamada `LocalAccountTokenFilterPolicy` com um valor de 1.

Para ajudar a evitar problemas que podem resultar de diferenças de fuso horário, use um servidor NTP para sincronizar fusos horários entre os recursos. Por exemplo, é possível sincronizar fusos horários para matrizes de armazenamento, hypervisors e servidores de aplicativos que estão em seu ambiente.

Se os fusos horários estiverem fora de sincronização, você pode encontrar erros durante tarefas de registro do aplicativo, catalogação de metadados, inventário, backup ou restauração ou restauração de arquivo. Para obter informações adicionais sobre como identificar e resolver o desvio do cronômetro, consulte [Tempo em desvios de máquina virtual devido ao desvio do cronômetro de hardware](#)

Considerações sobre o Hyper-V

Apenas volumes em discos SCSI são elegíveis para a catalogação de arquivos e restauração de arquivo.

Considerações do Linux

Se os dados estiverem localizados em volumes do LVM, o serviço `lvm2-lvmetad` deverá ser desativado, pois ele pode interferir com a capacidade do IBM Spectrum Protect Plus de montar e renunciar às capturas instantâneas ou clones do grupo de volumes. Para desativar o serviço, conclua as seguintes etapas:

1. Execute os seguintes comandos:

```
systemctl stop lvm2-lvmetad
```

```
systemctl disable lvm2-lvmetad
```

2. Edite o `/etc/lvm/lvm.conf` e especifique a seguinte configuração:

```
use_lvmetad = 0
```

Se os dados residirem em sistemas de arquivos XFS e a versão do pacote `xfspg` estiver entre 3.2.0 e 4.1.9, a restauração de arquivo pode falhar devido a um problema conhecido em `xfspg` que causa dano em um clone ou sistema de arquivos de captura instantânea quando seu UUID é modificado. Para resolver esse problema, atualize `xfspg` para a versão 4.2.0 ou acima. Para obter mais informações, consulte [Logs de relatório Debian Bug](#).

Procedimento

Para restaurar um arquivo, conclua as seguintes etapas.

1. Na área de janela de navegação, clique em **Gerenciar proteção > Restauração de arquivo**.
2. Insira uma sequência de procura para procurar um arquivo por nome e, em seguida, clique no ícone procurar . Para obter informações adicionais sobre como usar a função de procura, consulte Apêndice A, “Diretrizes de Procura”, na página 315.
3. Opcional: É possível usar filtros para otimizar sua procura em máquinas virtuais específicas, intervalo de data no qual o arquivo foi protegido e tipos de sistemas operacionais da máquina virtual. As procuras também podem ser limitadas a uma pasta específica por meio do campo **Caminho de pasta**. O campo **Caminho da Pasta** suporta curingas. Posicione os curingas no início, no meio ou no

final de uma sequência. Por exemplo, insira *Downloads para procurar na pasta Downloads sem inserir o caminho precedente.

4. Para restaurar o arquivo usando opções padrão, clique em **Restaurar**. O arquivo é restaurado para seu local original.
5. Para editar opções antes de restaurar o arquivo, clique em **Opções**. Configure as opções de restauração do arquivo.

Sobrescrever arquivos / pastas existentes

Substitua o arquivo ou pasta existente pelo arquivo ou pasta restaurada.

DESTINATION:

Selecione para substituir o arquivo ou pasta existente pelo arquivo ou pasta restaurada.

Para restaurar o arquivo para seu local original, selecione **Restaurar arquivos para o local original**.

Para restaurar para um destino local diferente do local original, selecione **Restaurar arquivos para local alternativo**. Em seguida, selecione o local alternativo a partir dos recursos disponíveis usando o menu de navegação ou a função de procura.

Restrição: Um arquivo pode ser restaurado para um local alternativo somente se as credenciais foram estabelecidas para a máquina virtual alternativa por meio da opção **Nome do usuário/Senha de S.O. guest** na definição de tarefa de backup.

Insira o caminho da pasta da máquina virtual no destino alternativo no campo **Pasta de destino**. Se o diretório não existir, ele será criado.

Clique em **Salvar** para salvar as opções.

6. Para restaurar o arquivo usando opções definidas, clique em **Restaurar**.

Tarefas relacionadas

[“Fazendo backup dos dados de VMware” na página 103](#)

Use uma tarefa de backup para fazer backup de recursos do VMware, como máquinas virtuais, armazenamentos de dados, pastas, vApps e data centers com capturas instantâneas.

[“Restaurando Dados do VMware” na página 111](#)

As tarefas de restauração do VMware suportam cenários de Restauração de VM instantânea e de Restauração de disco instantâneo, que são criados com base na origem selecionada.

Capítulo 8. Protegendo Aplicativos

Deve-se registrar os aplicativos de banco de dados que você deseja proteger no IBM Spectrum Protect Plus e, em seguida, criar tarefas para fazer backup e restaurar os bancos de dados e recursos que estão associados aos aplicativos.

Nota: O IBM Spectrum Protect Plus pode criar pastas em servidores de aplicativos quando os aplicativos são registrados no SPP. As pastas criadas pelo IBM Spectrum Protect Plus precisarão permanecer para que o produto funcione corretamente e não deverão ser removidas. Se houver uma necessidade de remover a pasta criada pelo SPP, cancele o registro do aplicativo no SPP. O SPP executará uma limpeza de pastas associadas ao registro.

Db2

Depois de incluir com sucesso instâncias do IBM Db2 no IBM Spectrum Protect Plus, é possível começar a proteger dados do Db2. Crie políticas de acordos de nível de serviço (SLA) para fazer backup e manter dados do Db2.

Certifique-se de que o ambiente Db2 atenda aos requisitos do sistema. Para obter mais informações, consulte [“Requisitos do Db2”](#) na página 31.

Dica: Se seus dados do Db2 forem armazenados em um ambiente multiparticionado com diversos hosts, será possível proteger seus dados do Db2 em cada host. Cada host no ambiente multiparticionado deve ser incluído no IBM Spectrum Protect Plus para que todas as instâncias e bancos de dados sejam detectados para proteção. Para obter mais informações, consulte [“Incluindo um servidor de aplicativos Db2”](#) na página 141.

Pré-requisitos para o Db2

Todos os pré-requisitos para o IBM Spectrum Protect Plus Servidor de aplicativos Db2 devem ser atendidos antes de você começar a proteger recursos do Db2 com o IBM Spectrum Protect Plus.

Os requisitos para o IBM Spectrum Protect Plus Servidor de aplicativos Db2 estão disponíveis aqui, [Requisitos do Db2](#).

Pré-requisitos de espaço

Certifique-se de que tenha espaço suficiente no sistema de gerenciamento de banco de dados Db2, nos grupos de volumes para a operação de backup e nos volumes de destino para copiar arquivos durante a operação de restauração. Para obter informações adicionais sobre requisitos de espaço, consulte [Requisitos de espaço para proteção do Db2](#). Quando estiver restaurando dados para um local alternativo, aloque volumes dedicados extras para os processos de cópia e restauração. Os caminhos de dados para espaços de tabela e logs no host de destino são iguais aos caminhos no host original. Essa configuração é necessária para permitir a cópia de dados do vSnap montado para o host de destino. Certifique-se de que os diretórios de banco de dados local dedicados sejam permitidos para cada banco de dados na configuração de volume.

Ambientes do Db2 multiparticionados

Para proteger os bancos de dados multiparticionados do Db2, o modo de backup do ACS deve ser configurado como modo paralelo. Para executar o processo de backup paralelo de partições em seu ambiente do Db2, assegure-se de que um dos pré-requisitos a seguir seja atendido:

- A variável de registro **DB2_PARALLEL_ACS** do Db2 está configurada como YES, por exemplo: **db2set DB2_PARALLEL_ACS=YES**.

- A variável de registro **DB2_WORKLOAD** do Db2 está configurada como SAP.

Restrição: A variável de registro **DB2_PARALLEL_ACS** está disponível apenas em determinados níveis de fix pack do Db2. Se **DB2_PARALLEL_ACS** não estiver disponível em sua versão, será possível optar por mudar **DB2_WORKLOAD** para SAP.

Mais requisitos de configuração

Certifique-se de que seu ambiente Db2 esteja configurado para atender aos seguintes critérios:

- A criação de log de archive do Db2 está ativada e o Db2 está no modo recuperável.
- Os espaços de tabelas do Db2 são separados dos arquivos de log com cada um em volumes lógicos dedicados que são gerenciados pelo Gerenciador de Volume Lógico (LVM2) Linux ou pelo AIX Journaling File System (JFS2).
- Certifique-se de que o tamanho do arquivo efetivo **ulimit -f** para o usuário do agente do IBM Spectrum Protect Plus e o usuário da instância do Db2 esteja configurado como unlimited. Como alternativa, configure o valor para um valor suficientemente alto para permitir a cópia dos maiores arquivos de banco de dados em suas tarefas de backup e de restauração. Se você mudar a configuração **ulimit**, reinicie a instância do Db2 para finalizar a configuração.
- Se estiver executando o IBM Spectrum Protect Plus em um ambiente AIX ou Linux, certifique-se de que a versão de sudo instalada esteja no nível recomendado. Para obter mais informações, consulte a nota técnica 2013790. Em seguida, configure privilégios sudo conforme descrito em “Configurando privilégios sudo para Db2” na página 140.
- Em um ambiente Linux, assegure-se de que o pacote do utilitário Linux, **util-linux-ng**, ou o pacote **util-linux** seja atual.
- Certifique-se de que o serviço SSH esteja em execução na porta 22 no servidor e que os firewalls estejam configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor com SSH. O subsistema SFTP para SSH deve ser ativado.
- Os caracteres Unicode em nomes de caminhos de arquivo não podem ser manipulados por IBM Spectrum Protect Plus. Todos os nomes devem estar em ASCII.
- Os espaços de tabela de banco de dados, os logs on-line e o diretório de banco de dados local podem estar em um ou em volumes lógicos dedicados separados que são gerenciados pelo LVM2 ou JFS2. Para dois exemplos de layout, consulte as figuras a seguir. Na primeira figura, são mostrados dois tipos de grupos de volumes. Na segunda figura, todos os volumes para dados e logs estão em um grupo de volumes.

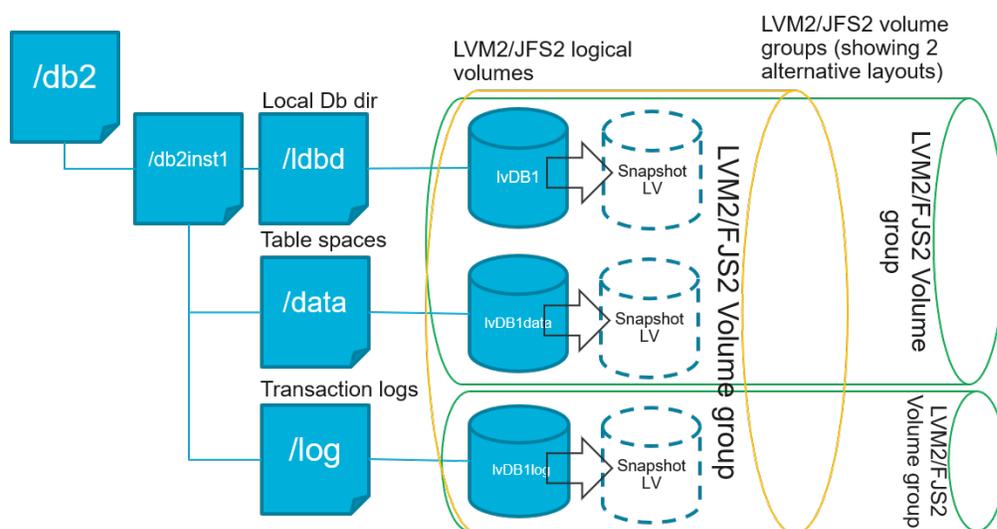


Figura 13. Exemplos de Layout de Volume Lógico

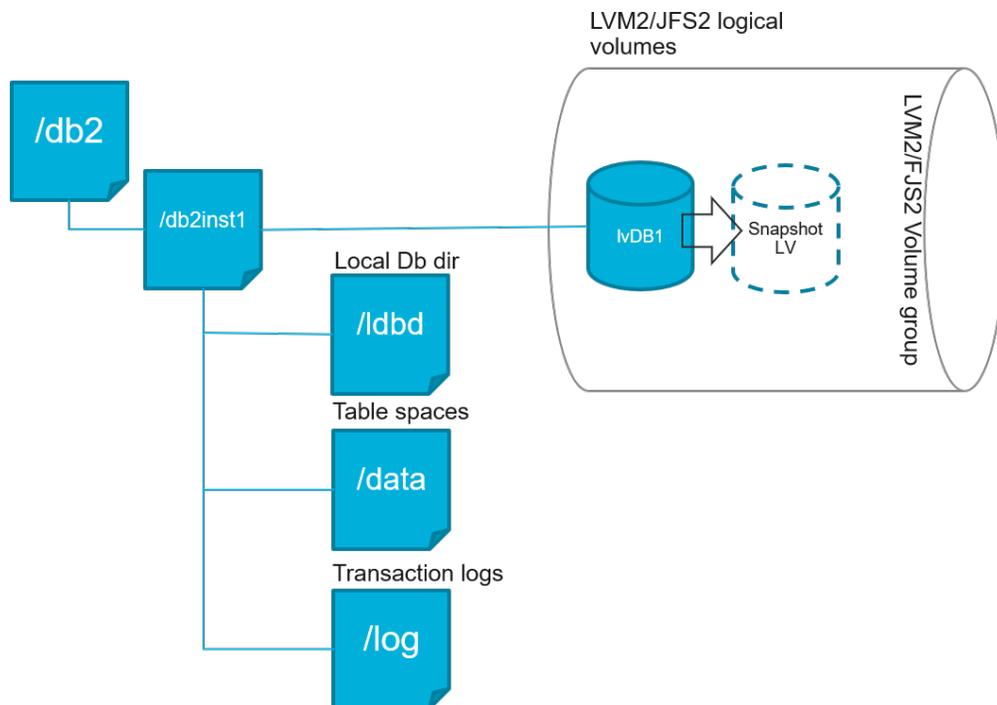


Figura 14. Exemplo de Layout de Volume Lógico Único

- Certifique-se de que a configuração de volume lógico do Db2 não inclua pontos de montagem aninhados.

Requisitos de Espaço para Proteção Db2

Antes de iniciar o backup de bancos de dados Db2, certifique-se de que tenha espaço livre em disco suficiente nos hosts de destino e de origem, e no repositório do vSnap. É necessário que haja espaço livre em disco adicional nos grupos de volumes no host de origem para a criação de capturas instantâneas de Gerenciador de volume lógico (LVM) temporárias dos volumes lógicos nos quais os arquivos de log e de banco de dados do Db2 estão armazenados. Para criar capturas instantâneas do LVM de um banco de dados Db2 protegido, certifique-se de que os grupos de volumes com dados do Db2 tenham espaço livre suficiente.

Capturas instantâneas do LVM

Capturas instantâneas do LVM são cópias point-in-time de volumes lógicos do LVM. Elas são capturas instantâneas com espaço eficiente com as atualizações de dados mudados do volume lógico de origem. As capturas instantâneas do LVM são criadas no mesmo grupo de volumes que o volume lógico de origem. O agente do IBM Spectrum Protect Plus Db2 usa capturas instantâneas do LVM para criar uma cópia point-in-time temporária, consistente do banco de dados Db2.

O agente do IBM Spectrum Protect Plus Db2 cria uma captura instantânea do LVM que é então montada e copiada para o repositório do vSnap. A duração da operação de cópia de arquivo depende do tamanho do banco de dados Db2. Durante a cópia de arquivo, o aplicativo Db2 permanece totalmente on-line. Após a conclusão da operação de cópia de arquivo, as capturas instantâneas do LVM são removidas pelo agente do IBM Spectrum Protect Plus Db2 em uma operação de limpeza.

Para AIX, não podem existir mais de 15 capturas instantâneas para cada sistema de arquivos JFS2. As capturas instantâneas JFS2 internas e externas não podem existir ao mesmo tempo para o mesmo sistema de arquivos. Certifique-se de que não existam capturas instantâneas internas nos volumes JFS2, pois essas capturas instantâneas podem causar problemas quando o agente do Db2 do IBM Spectrum Protect Plus estiver criando capturas instantâneas externas.

Para cada volume lógico de captura instantânea do LVM ou JFS2 que contém dados, deixe pelo menos 10 por cento de seu tamanho como espaço livre em disco no grupo de volumes. Se o grupo de volumes tiver

espaço livre em disco suficiente, o agente do IBM Spectrum Protect Plus Db2 reservará até 25 por cento do tamanho do volume lógico de origem para o volume lógico de captura instantânea.

LVM2 e JFS2

Quando uma operação de backup do Db2 é executada, o Db2 solicita uma captura instantânea. Esta captura instantânea é criada em um sistema Logical Volume Management (LVM) ou em um Sistema de Arquivos Registrados (JFS) para cada volume lógico com dados ou logs para o banco de dados selecionado. Em sistemas Linux, os volumes lógicos são gerenciados pelo LVM2 com comandos `lvm2`. No AIX, os volumes lógicos são gerenciados pelo JFS2 e criados com o comando de captura instantânea JFS2 como capturas instantâneas externas.

Uma captura instantânea LVM2 ou JFS2 baseada em software é obtida como um novo volume lógico no mesmo grupo de volumes. Os volumes de captura instantânea são montados temporariamente na mesma máquina que executa a instância do Db2 para que eles possam ser transferidos para o repositório do vSnap.

No sistema operacional Linux, o gerenciador de volume LVM2 armazena a captura instantânea de um volume lógico dentro do mesmo grupo de volumes. No sistema operacional AIX, o gerenciador de volume JFS2 armazena a captura instantânea de um volume lógico dentro do mesmo grupo de volumes. Para ambos, deve haver espaço suficiente na máquina para armazenar o volume lógico. O volume lógico aumenta em tamanho conforme os dados são mudados no volume de origem enquanto a captura instantânea existe. Em ambientes multiparticionados, quando várias partições compartilham o mesmo volume, uma captura instantânea extra do volume é criada para cada partição. Assegure-se de que o grupo de volumes tenha espaço livre suficiente para as capturas instantâneas necessárias.

Configurando privilégios sudo para Db2

Para usar o IBM Spectrum Protect Plus para proteger seus dados, você deve instalar a versão necessária do programa sudo. Para o servidor de aplicativos Db2, deve-se configurar sudo de uma forma específica que pode ser diferente dos outros servidores de aplicativos.

Antes de Iniciar

Para determinar a versão correta de sudo a ser instalada, consulte a nota técnica [2013790](#).

Sobre Esta Tarefa

Configure um usuário do agente dedicado do IBM Spectrum Protect Plus com os privilégios de superusuário necessários para sudo. Essa configuração permite que o usuário do agente execute comandos sem uma senha.

Procedimento

1. Crie um usuário do servidor de aplicativos emitindo o seguinte comando:

```
useradd -m <agent>
```

em que `agent` especifica o nome do usuário do agente do IBM Spectrum Protect Plus.

2. Configure uma senha para o novo usuário emitindo o seguinte comando:

```
passwd <agent>
```

3. Para ativar privilégios de superusuário para o usuário do agente, defina a configuração `!requiretty`. No final do arquivo de configuração sudo, inclua as seguintes linhas:

```
Defaults: < agent>! requiretty
< agent> ALL = (ALL) NOPASSWD:ALL
```

Se o arquivo `sudoers` estiver configurado para importar configurações de outro diretório, por exemplo, `/etc/sudoers.d`, é possível incluir as linhas no arquivo apropriado nesse diretório.

Incluindo um servidor de aplicativos Db2

Para começar a proteger os dados do Db2, deve-se incluir o endereço do host no qual as instâncias do Db2 estão localizadas. É possível repetir o procedimento para incluir cada host que você deseja proteger com o IBM Spectrum Protect Plus. Caso o ambiente do Db2 seja multiparticionado com vários hosts, deve-se incluir cada host no IBM Spectrum Protect Plus.

Sobre Esta Tarefa

Para incluir um servidor de aplicativos Db2 no IBM Spectrum Protect Plus, deve-se ter o endereço do host da máquina.

Procedimento

1. Na navegação, expanda **Gerenciar proteção > Aplicativos > Db2**.
2. Na janela **Db2**, clique em **Gerenciar servidores de aplicativos** e clique em **Incluir servidor de aplicativos** para incluir a máquina host.



Figura 15. Incluindo um agente do Db2

3. Na seção **Propriedades do aplicativo**, insira o endereço do host.
4. Escolha especificar um usuário ou usar uma chave SSH.
 - Se você selecionou para especificar um usuário, selecione um usuário existente ou insira um ID do usuário e senha.
 - Se estiver usando uma chave SSH, escolha a chave a partir do menu.

Nota: O usuário deve ter privilégios sudo configurados.

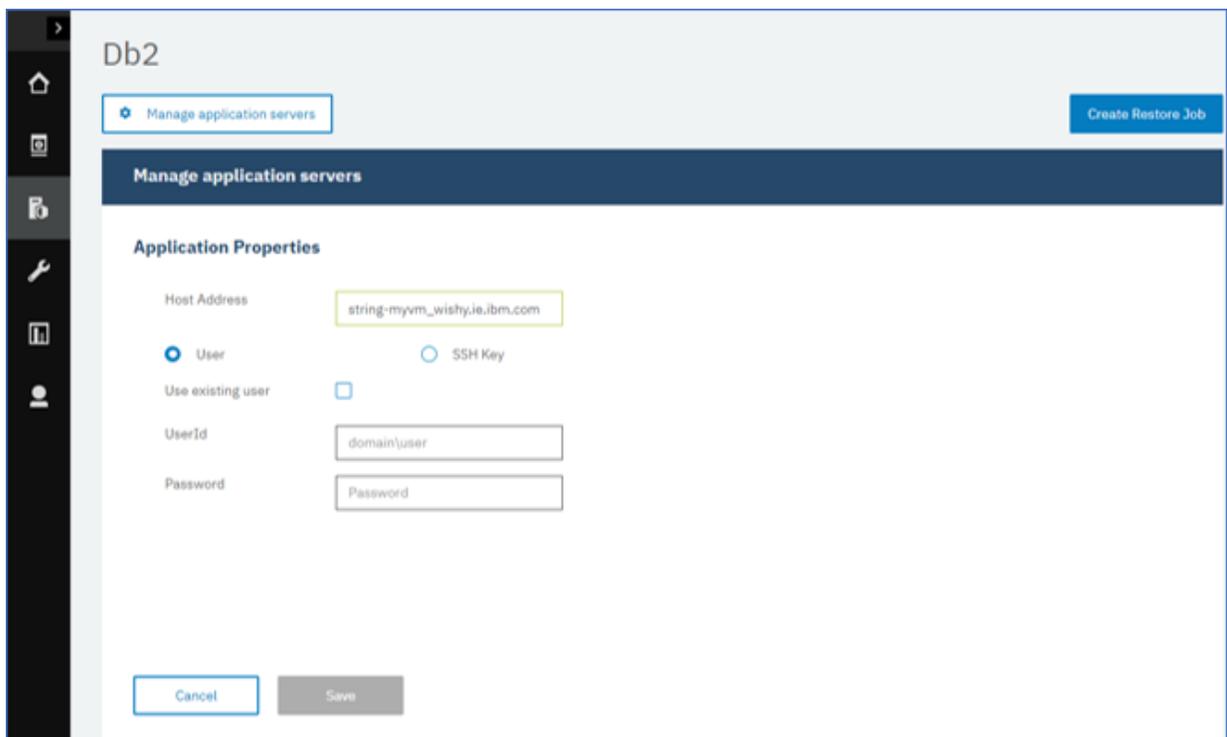


Figura 16. Gerenciando usuários do agente

Dica:

As instâncias do Db2 localizadas são listadas para cada host. Se a instância do Db2 for particionada, essa informação será listada com a máquina host e os números das partições. Para o DPF (Database Partitioning Feature) com vários hosts, a instância do Db2 é exibida como uma única unidade.

5. Clique em **Obter instâncias** para listar as instâncias do Db2 disponíveis.
6. Salve o formulário e repita as etapas para incluir outros servidores de aplicativos Db2 no IBM Spectrum Protect Plus.

Se os seus dados do Db2 estiverem em um ambiente multiparticionado com vários hosts, será necessário incluir cada host. Repita o procedimento para cada host Db2.

O que Fazer Depois

Depois de incluir seus servidores de aplicativos Db2 no IBM Spectrum Protect Plus, um inventário é executado automaticamente em cada servidor de aplicativos para detectar os bancos de dados relevantes nessas instâncias.

Para verificar se os bancos de dados foram incluídos, revise o log da tarefa. Acesse **Tarefas e operações**. Clique na guia **Tarefas em execução** e procure a entrada de log Inventário do servidor de aplicativos mais recente.

As tarefas concluídas são mostradas na guia **Histórico da tarefa**. É possível usar a lista **Classificar por** para classificar tarefas com base no horário de início, no tipo, no status, no nome ou na duração da tarefa. Use o campo **Procurar por nome** para procurar tarefas por nome. É possível utilizar asteriscos como caracteres curinga no nome.

Os bancos de dados devem ser detectados para assegurar que possam estar protegidos. Para obter instruções sobre como executar um inventário, consulte [Detectando recursos do Db2](#).

Detectando recursos do Db2

Depois de incluir servidores de aplicativos IBM Db2 no IBM Spectrum Protect Plus, um inventário para detectar todas as instâncias e bancos de dados do Db2 é executado automaticamente. O inventário detecta, lista e armazena todos os bancos de dados Db2 para o host selecionado e disponibiliza os bancos de dados para proteção com o IBM Spectrum Protect Plus.

Antes de Iniciar

Certifique-se de que tenha incluído servidores de aplicativos Db2 no IBM Spectrum Protect Plus. Para obter instruções, consulte [Incluindo um servidor de aplicativos do Db2](#).

Sobre Esta Tarefa

Todas as partições do Db2 que estão localizadas no inventário são listadas para a instância do Db2. As partições são listadas pelo seus números de partição de cada host anexado ao nome do host na tabela **Instâncias**.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Db2**.

Dica: Para incluir mais instâncias Db2 na área de janela **Instâncias**, siga as instruções em [Incluindo um servidor de aplicativos do Db2](#).

2. Clique em **Executar inventário**.

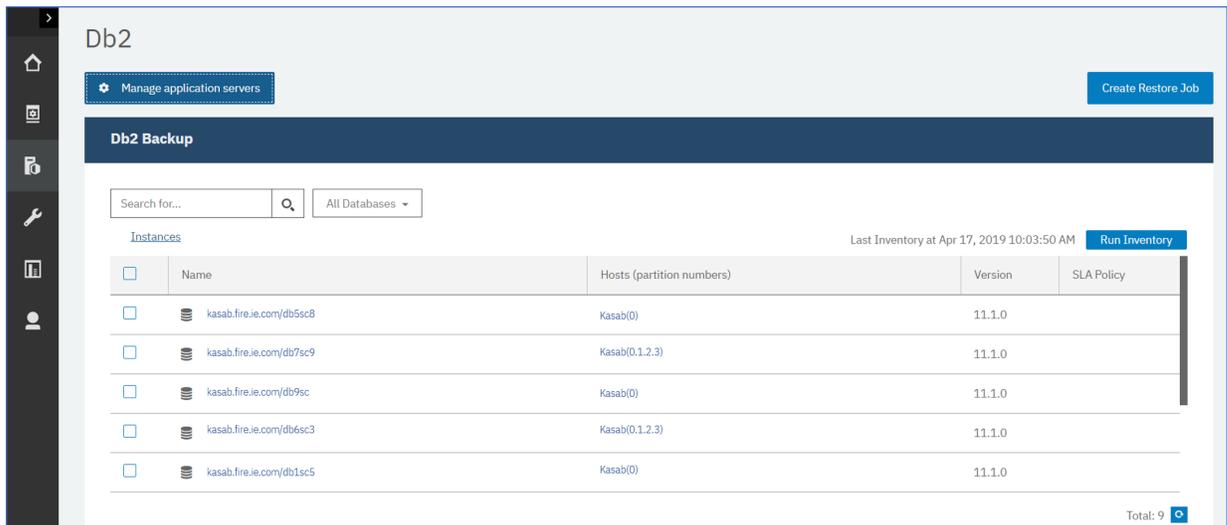


Figura 17. Detectando recursos do Db2

Quando o inventário estiver em execução, o botão mudará para mostrar **Inventário em andamento**. É possível executar um inventário em quaisquer servidores de aplicativos disponíveis, mas é possível executar somente um processo de inventário por vez.

Para visualizar o log da tarefa, acesse **Tarefas e operações**. Clique na guia **Tarefas em execução** e procure a entrada do log Inventário do servidor de aplicativos mais recente.

As tarefas concluídas são mostradas na guia **Histórico da tarefa**. É possível usar a lista **Classificar por** para classificar tarefas com base no horário de início, no tipo, no status, no nome ou na duração da tarefa. Use o campo **Procurar por nome** para procurar tarefas por nome. É possível utilizar asteriscos como caracteres curinga no nome.

3. Clique em uma instância para abrir uma visualização que mostra os bancos de dados que são detectados para essa instância. Se algum banco de dados estiver ausente da lista **Instâncias**, verifique o servidor de aplicativos Db2 e execute novamente o inventário. Em alguns casos, alguns bancos de dados são marcados como ilegíveis para backup; passe o mouse sobre o banco de dados para revelar a razão disso.

Dica: Para retornar à lista de instâncias, clique no hipertexto **Instâncias** na área de janela **Fazer backup do Db2**.

O que Fazer Depois

Para começar a proteger os bancos de dados Db2 que estão catalogados na instância selecionada, aplique uma política de acordo de nível de serviço (ANS) à instância. Para obter instruções sobre como configurar uma política de ANS, consulte [Definindo uma política de ANS](#).

Testando a conexão Db2

Depois de incluir um servidor de aplicativos Db2, é possível testar a conexão. O teste verifica a comunicação com o servidor e as configurações de DNS entre o IBM Spectrum Protect Plus e o servidor Db2. Ele também verifica as permissões de sudo corretas para o usuário.

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Db2**.
2. Na janela **Db2**, clique em **Gerenciar servidores de aplicativos** e selecione o **Endereço do host** que você deseja testar.
É mostrada uma lista dos servidores de aplicativos Db2 que estão disponíveis.
3. Clique em **Ações** e escolha **Testar** para iniciar os testes de verificação para conexões e configurações físicas, remotas e do sistema operacional.

Test result of kasab5

1. Physical - Basic Test for physical host network configuration

Name	Description	Status	Message
Host FQDN Resolvable Test	Host FQDN must be resolvable to an IPv4 address	✓	
Socket Connection Test	Must allow socket connection on port 22 for Linux	✓	

2. Remote - Remote executor test for session creation and remote agent deployment

Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient privileges.	✓	

3. AIX - Basic AIX prerequisites for file and volume operations

Name	Description	Status	Message
Sudo Privileges	User must have password-less sudo privileges	✓	

Figura 18. Testando a conexão

O relatório de teste mostra uma lista dos testes. Ele consiste em um teste para a configuração de rede do host físico e testa a instalação do servidor remoto no host, que verifica SSH e SFTP no host. O terceiro teste verifica os pré-requisitos do sistema operacional e os privilégios corretos de sudo.

4. Clique em **OK** para fechar o teste e escolha executar novamente o teste depois de corrigir quaisquer testes com falha.

Fazendo backup de dados do Db2

Defina tarefas de backup regulares do Db2 com opções para executar e criar cópias de backup para proteger seus dados. É possível ativar o backup contínuo de logs de archive para que seja possível restaurar uma cópia point-in-time com opções de rollforward, se necessário.

Antes de Iniciar

Durante o backup inicial, o IBM Spectrum Protect Plus cria um novo volume do vSnap e compartilhamento de NFS. Durante backups incrementais, o volume criado anteriormente é reutilizado. O agente do IBM Spectrum Protect Plus Db2 monta o compartilhamento no servidor Db2 no qual o backup deve ser concluído.

Revise os seguintes procedimentos e considerações antes de criar uma definição de tarefa de backup:

- Inclua os servidores de aplicativos dos quais você deseja fazer backup. Para o procedimento, consulte [Incluindo um servidor de aplicativos Db2](#).

- Configure uma Política de Acordo de Nível de Serviço (ANS). Para o procedimento, consulte [Definindo uma tarefa de backup de Acordo de Nível de Serviço](#).
- Antes de um usuário do IBM Spectrum Protect Plus poder implementar operações de backup e restauração, as funções e grupos de recursos devem ser designados ao usuário. Conceda aos usuários acesso a recursos e a operações de backup e restauração por meio da área de janela **Contas**. Para obter mais informações, veja [Gerenciando o acesso de usuário](#).
- As tarefas de inventário não devem ser planejadas para serem executadas ao mesmo tempo que as tarefas de backup.
- Evite configurar backups do log para um único banco de dados Db2 com muitas tarefas de backup. Se um único banco de dados Db2 for incluído em várias definições de tarefa com o backup do log ativado, um backup do log de uma tarefa poderá truncar um log antes de ele ser submetido a backup pela próxima tarefa. Isso pode causar falha das tarefas de restauração point-in-time.

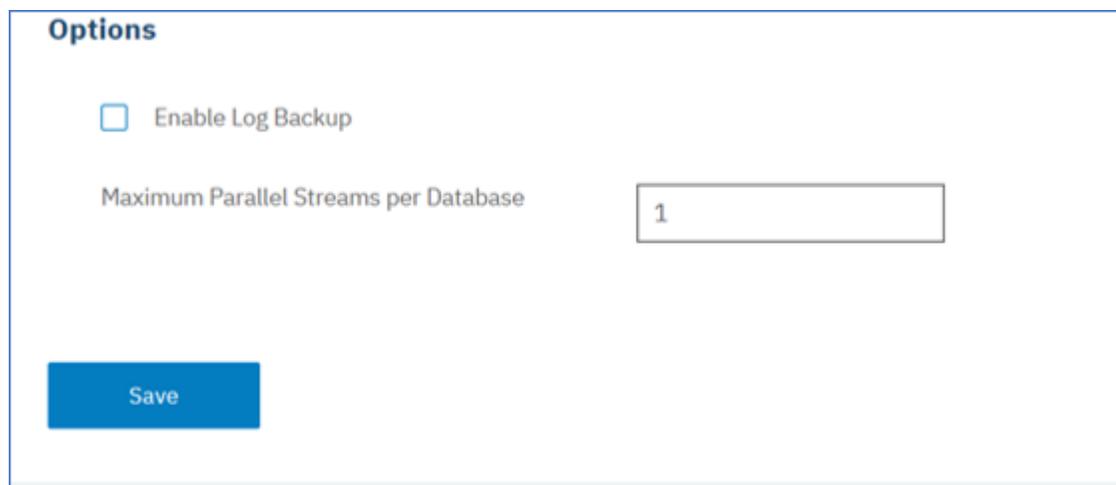
Procedimento

1. No menu de navegação, expanda **Gerenciar proteção > Aplicativos > Db2**.
2. Selecione uma instância ou banco de dados para backup escolhendo uma das seguintes ações:
 - Selecione uma instância inteira na área de janela **Instâncias**, clicando na caixa de seleção ao lado do nome da instância. Todos os bancos de dados incluídos nessa instância são automaticamente designados à política de ANS escolhida.
 - Selecione um banco de dados específico em uma instância clicando no nome da instância e escolhendo um banco de dados a partir da lista de bancos de dados nessa instância.

Cada item na área de janela **Instâncias** é listado por nome de instância ou de banco de dados, pela política de ANS aplicada e a elegibilidade para backup do log.

3. Clique em **Selecionar opções** para ativar ou desativar o backup do log e especificar fluxos paralelos para reduzir o tempo gasto para movimentação de dados grandes na operação de backup. Clique em **Salvar** para confirmar as opções.

Selecione **Ativar backup de log** para fazer backup de logs de archive, o que permite opções de restauração e opções de recuperação de momento. Para obter informações de configurações de backup do log do Db2, consulte [Backups do log](#).



The image shows a dialog box titled "Options" with a light blue header. Inside the dialog, there is a checkbox labeled "Enable Log Backup" which is currently unchecked. Below this, there is a text input field labeled "Maximum Parallel Streams per Database" containing the number "1". At the bottom left of the dialog is a blue button labeled "Save".

Figura 19. Área de janela Backup com a opção Ativar backup do log

Ao salvar as opções, essas opções são usadas para todas as tarefas de backup para este banco de dados ou instância conforme selecionado.

4. Selecione o banco de dados ou instância novamente e clique em **Selecionar política de ANS** para escolher uma política de ANS para esse banco de dados ou instância.

5. Salve as opções do SLA.

Para definir um novo ANS ou editar uma política existente com taxas de retenção e frequência customizadas, selecione **Gerenciar proteção > Visão geral de política**. Na área de janela **Políticas de ANS**, clique em **Incluir política de ANS** e defina suas preferências de política.

O que Fazer Depois

Quando a política de ANS for salva, se você escolher, pode executar um backup on-demand a qualquer momento, clicando em **Ações**, ao lado do nome da política e selecionando **Iniciar**. O status no log muda para mostrar que o backup está Running.

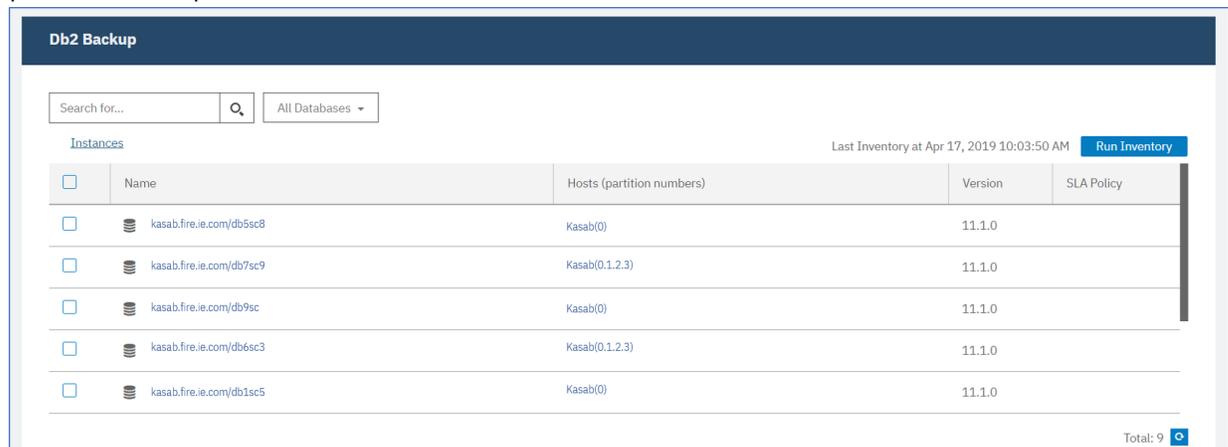
Definindo uma tarefa de backup de acordo de nível de serviço

Quando os bancos de dados Db2 estiverem listados para cada uma das instâncias do Db2, selecione e aplique uma política de acordo de nível de serviço (ANS) para começar a proteger seus dados.

Procedimento

1. No menu de navegação, expanda **Gerenciar proteção > Aplicativos > Db2**.
2. Selecione uma instância do Db2 para fazer backup de todos os dados nessa instância ou clique no nome da instância para visualizar os bancos de dados disponíveis para backup. Em seguida, é possível selecionar bancos de dados individuais na instância do Db2 que você deseja fazer backup.

Escolha para fazer backup de uma instância inteira com todos os dados associados ou é possível optar por fazer backup de um ou mais bancos de dados.



The screenshot shows the 'Db2 Backup' interface. At the top, there is a search bar and a dropdown menu for 'All Databases'. Below this is a table with the following columns: 'Name', 'Hosts (partition numbers)', 'Version', and 'SLA Policy'. The table lists five instances of Db2 databases. At the bottom right, there is a 'Total: 9' indicator.

	Name	Hosts (partition numbers)	Version	SLA Policy
<input type="checkbox"/>	kasab.fire.ie.com/db5sc8	Kasab(0)	11.1.0	
<input type="checkbox"/>	kasab.fire.ie.com/db7sc9	Kasab(0.1.2.3)	11.1.0	
<input type="checkbox"/>	kasab.fire.ie.com/db9sc	Kasab(0)	11.1.0	
<input type="checkbox"/>	kasab.fire.ie.com/db6sc3	Kasab(0.1.2.3)	11.1.0	
<input type="checkbox"/>	kasab.fire.ie.com/db1sc5	Kasab(0)	11.1.0	

Figura 20. Área de janela de backup do Db2 mostrando instâncias

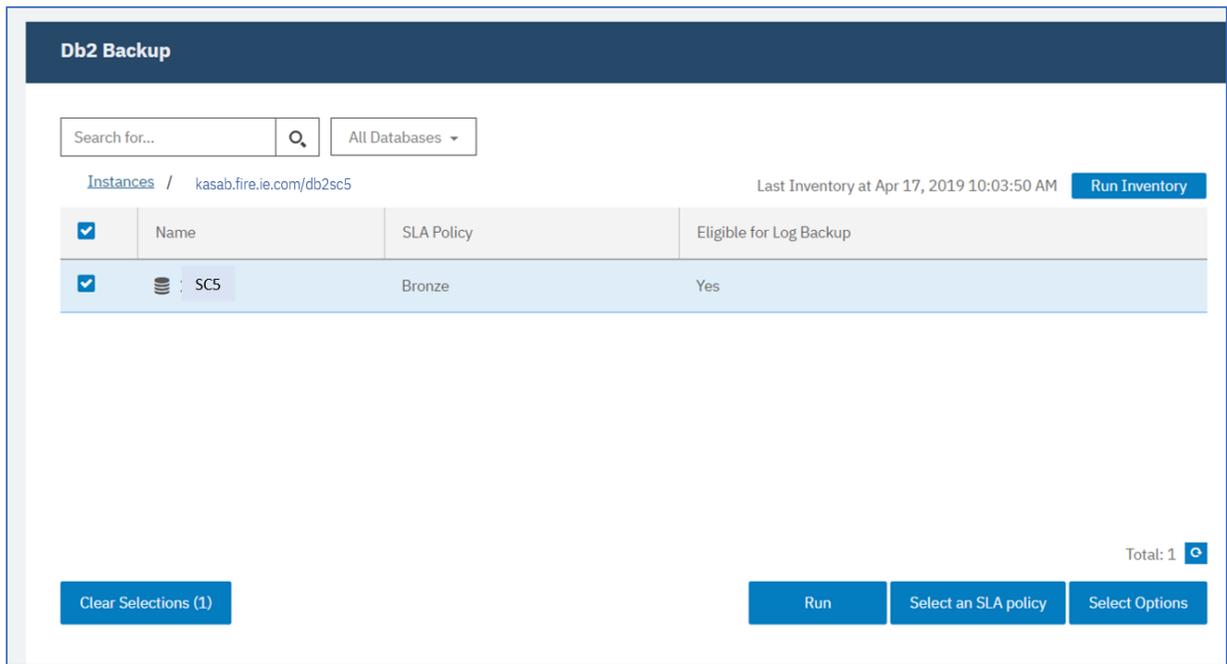


Figura 21. Área de janela Backup do Db2 que mostra bancos de dados em uma instância

3. Clique em **Selecionar política de ANS** e escolha uma política de ANS, **Ouro**, **Prata** ou **Bronze**. Salve sua opção.

As opções predefinidas de Ouro, Prata ou Bronze, cada uma tem frequências e taxas de retenção diferentes. É possível criar uma política de ANS customizada ou editar uma política existente, navegando para **Visão geral de política > Políticas de ANS**.

4. Clique em **Selecionar opções** para definir opções para seu backup, como ativar backups de log para futuras opções de recuperação e especificar os fluxos paralelos para reduzir o tempo gasto para fazer backup de bancos de dados grandes. Salve suas mudanças.

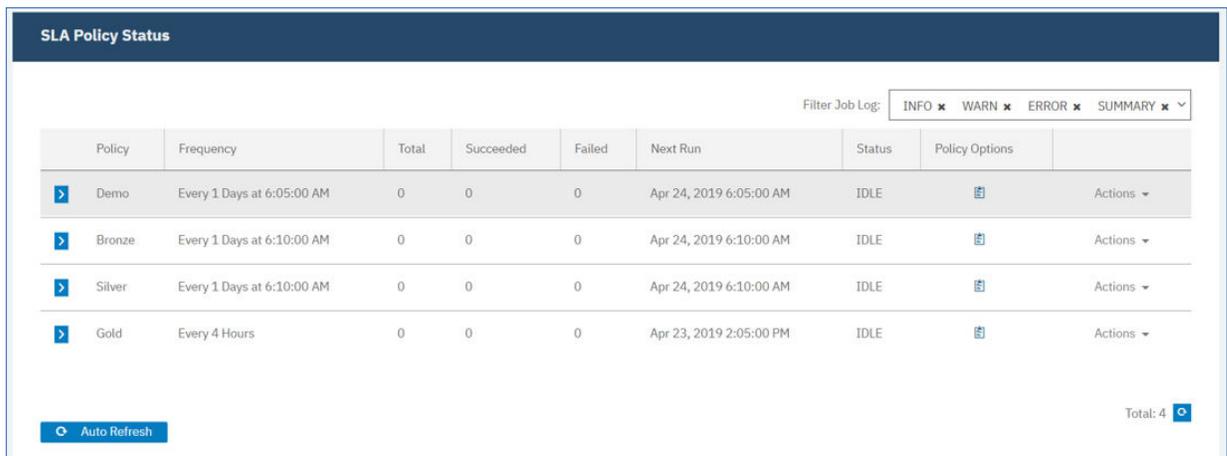


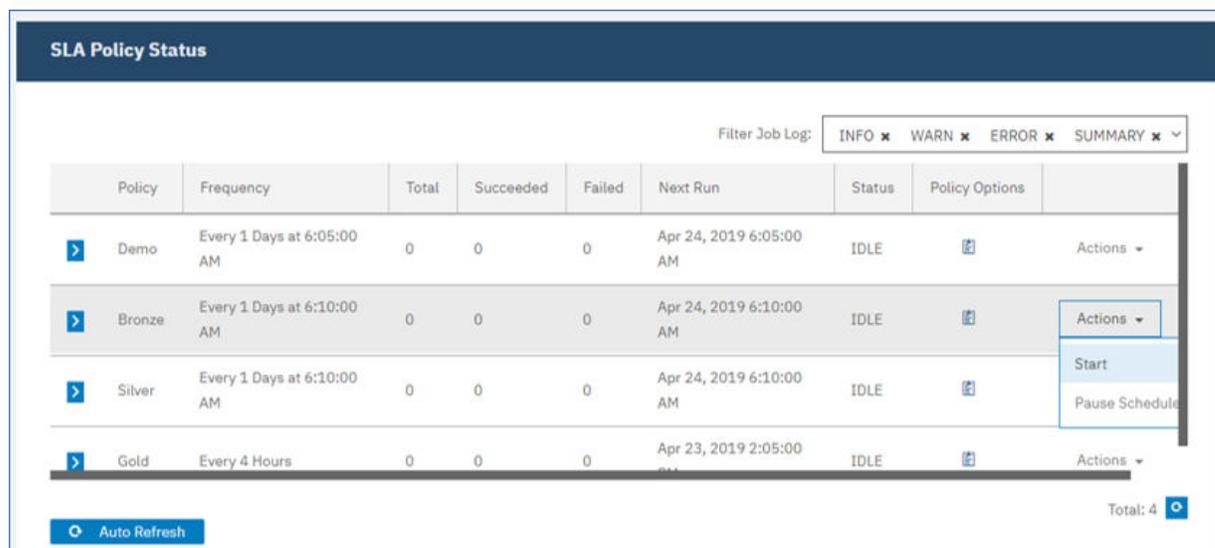
Figura 22. Opções de Backup e Políticas de SLA

5. Configure a política de ANS clicando no ícone na coluna **Opções de política** da tabela **Status de política de ANS**.

Para ler sobre mais opções de configuração de ANS, consulte [“Configurando opções de configuração de ANS para uma tarefa de backup”](#) na página 148.

6. Se você desejar executar a política fora da tarefa planejada, selecione a instância ou banco de dados. Clique em **Ações** e selecione **Iniciar**.

O status muda para **Em execução** para seu ANS escolhido e é possível acompanhar o progresso da tarefa no log da tarefa mostrado.



The screenshot displays the 'SLA Policy Status' interface. At the top, there is a 'Filter Job Log' section with buttons for 'INFO', 'WARN', 'ERROR', and 'SUMMARY'. Below this is a table with columns: Policy, Frequency, Total, Succeeded, Failed, Next Run, Status, Policy Options, and Actions. The table lists four policies: Demo, Bronze, Silver, and Gold. All policies are currently in an 'IDLE' status. The 'Actions' column for each policy has a dropdown menu that is open for the 'Bronze' policy, showing options like 'Start' and 'Pause Schedule'. At the bottom left, there is an 'Auto Refresh' button, and at the bottom right, it shows 'Total: 4'.

Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	Actions
Demo	Every 1 Days at 6:05:00 AM	0	0	0	Apr 24, 2019 6:05:00 AM	IDLE		Actions
Bronze	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions
Silver	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions
Gold	Every 4 Hours	0	0	0	Apr 23, 2019 2:05:00 AM	IDLE		Actions

Figura 23. Políticas de SLA

Para pausar o planejamento de um ANS, clique em **Ações** e escolha **Parar planejamento**.

Para cancelar uma tarefa após ela ter sido iniciada, clique em **Ações > Cancelar**.

Configurando opções de configuração de ANS para uma tarefa de backup

Depois de configurar um acordo de nível de serviço, (ANS), para sua tarefa de backup, é possível optar por configurar mais opções para essa tarefa. É possível executar scripts, excluir recursos da operação de backup e forçar uma cópia de backup de base completo de um banco de dados, se necessário.

Procedimento

1. Na coluna **Opções de política** da tabela **Status da política de ANS** para a tarefa que está sendo

configurada, clique no ícone da área de transferência  para especificar opções extras de configuração.

Se a tarefa já estiver configurada, clique no ícone para editar a configuração.

Figura 24. Especificando Opções de Configuração do SLA

2. Clique em **Pré-script** e defina sua configuração de pré-script escolhendo uma das seguintes opções:
 - Clique em **Usar servidor de script** e selecione um script transferido por upload do menu.
 - Não clique em **Usar Servidor de Script** . Selecione um servidor de aplicativos da lista para executar o script nesse local.
3. Clique em **Pós-script** e defina sua configuração de pós-script escolhendo uma das seguintes opções:
 - Clique em **Usar servidor de script** e selecione um script transferido por upload do menu.
 - Não clique em **Usar Servidor de Script** . Selecione um servidor de aplicativos da lista para executar o script nesse local.

Os scripts e servidores de script são configurados na página **Configuração do sistema > Script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#).

4. Para continuar executando a tarefa quando o script associado à tarefa falhar, selecione **Continuar a tarefa durante erro do script**.

Se essa opção estiver selecionada, a operação de backup ou de restauração será tentada novamente e o status da tarefa de script será relatado como COMPLETED quando o script concluir o processamento com um código de retorno diferente de zero. Se esta opção não estiver selecionada, não haverá nova tentativa de backup ou restauração e o status da tarefa de script será relatado como COM FALHA.
5. Para excluir recursos de uma tarefa de backup, especifique os recursos a serem excluídos da tarefa. Insira um nome de recurso exato no campo **Excluir recursos**. Se não tiver certeza de um nome, use asteriscos curinga que são especificados antes do padrão (**text*) ou depois do padrão (*text**). Vários curingas podem ser inseridos com caracteres alfanuméricos padrão e os seguintes caracteres especiais: - _ e *. Separe as entradas com um ponto-e-vírgula.
6. Para criar um novo backup completo de um recurso, insira o nome desse recurso no campo **Forçar backup completo de recursos**. Separe vários recursos com um ponto-e-vírgula.

O backup completo cria um novo backup completo desse recurso e substitui o backup existente desse recurso apenas para uma ocorrência. Após a conclusão do backup completo, o recurso é submetido a backup incremental como antes.

Backups de log

Os logs arquivados para os bancos de dados contêm dados de transação confirmados. Esses dados de transação podem ser usados para executar um Rollforward de recuperação de dados quando você estiver executando uma operação de restauração. O uso de backups de log de archive aprimora o objetivo do ponto de recuperação para seus dados.

Certifique-se de selecionar a opção **Ativar backups do log** para permitir o Rollforward de recuperação ao configurar uma tarefa de backup ou política de acordo de nível de serviço (ANS). Quando selecionado pela primeira vez, deve-se executar uma tarefa de backup para a política de ANS para ativar o arquivamento de log no IBM Spectrum Protect Plus no banco de dados. Esse backup cria um volume separado no repositório vSnap, que é montado de maneira persistente no servidor de aplicativos Db2. O processo de backup atualiza os parâmetros **LOGARCHMETH1** ou **LOGARCHMETH2** para apontar para esse volume para propósitos de arquivamento de log. O volume é mantido montado no servidor de aplicativos Db2, a menos que a opção **Ativar backup de log** esteja desmarcada e uma nova tarefa de backup seja executada.

Restrição: Em ambientes multiparticionados do Db2, os parâmetros **LOGARCHMETH** nas partições devem corresponder.

Quando os parâmetros **LOGARCHMETH1** ou **LOGARCHMETH2** forem configurados com um valor diferente de OFF, será possível usar logs arquivados para um Rollforward de recuperação. É possível cancelar tarefas de backup do log a qualquer momento limpando a opção **Ativar backups do log**: acesse **Gerenciar proteção > Aplicativos > Db2**, selecione a instância e clique em **Selecionar opções**. Esta mudança entra em vigor após a conclusão bem-sucedida da próxima tarefa de backup, e o valor de parâmetro **LOGARCHMETH** muda de volta para sua configuração original.

Importante: O IBM Spectrum Protect Plus pode ativar tarefas de backup de log apenas quando o parâmetro **LOGARCHMETH1** está configurado como LOGRETAIN ou se um dos parâmetros **LOGARCHMETH** está configurado como OFF.

Se o parâmetro LOGARCHMETH1 estiver configurado como LOGRETAIN.

O IBM Spectrum Protect Plus muda o valor de parâmetro **LOGARCHMETH1** para ativar backups do log.

Se o parâmetro LOGARCHMETH1 ou LOGARCHMETH2 estiver configurado como OFF e o outro estiver configurado como DISK, TSM ou VENDOR.

O IBM Spectrum Protect Plus usa o parâmetro **LOGARCHMETH** que está configurado como off para ativar backups do log.

Se ambos os parâmetros LOGARCHMETH estiverem configurados como DISK, TSM ou VENDOR.

Essa combinação de configuração causa um erro quando o IBM Spectrum Protect Plus tenta ativar backups do log. Para resolver o erro, configure um dos parâmetros como OFF e execute a tarefa de backup com a opção **Ativar backups do log** selecionada.

Truncamento de backups de log de archive

O IBM Spectrum Protect Plus exclui automaticamente os logs transacionais mais antigos após um backup de banco de dados bem-sucedido. Essa ação assegura que a capacidade do volume de archive de log não seja comprometida pela retenção de arquivos de log mais antigos. Esses arquivos de log truncados são armazenados no repositório do vSnap até que o backup correspondente expire e seja excluído. A retenção de backups de banco de dados é definida na política de ANS selecionada. Para obter informações adicionais sobre políticas de ANS, consulte [“Definindo uma tarefa de backup de acordo de nível de serviço” na página 146](#).

O IBM Spectrum Protect Plus não gerencia a retenção de outros locais de logs arquivados.

Para obter informações adicionais sobre configurações do Db2, consulte a [página de Boas-vindas do IBM Db2](#).

Restaurando Dados do Db2

Para restaurar dados do Db2 do repositório do vSnap, defina uma tarefa que restaure dados do backup mais recente ou de uma cópia de backup anterior. É possível optar por restaurar dados para a instância original ou para uma instância alternativa em uma máquina diferente e especificar opções de recuperação e salvar a tarefa.

Antes de Iniciar

Importante: Para todas as operações de restauração, o Db2 deve estar no mesmo nível de versão nos hosts de origem e de destino. Além desse requisito, deve-se assegurar que uma instância com o mesmo nome que a instância que está sendo restaurada exista em cada host. Esse requisito se aplica quando a instância de destino tem o mesmo nome e quando os nomes são diferentes. Para que a operação de restauração seja bem-sucedida, ambas as instâncias devem ser provisionadas, uma com o nome original e a outra com o novo nome.

Se o seu ambiente Db2 incluir bancos de dados particionados, os dados de todas as partições serão submetidos a backup durante tarefas de backup regulares. Todas as instâncias são listadas na área de janela de backup. As instâncias multiparticionadas são mostradas com números de partição e nomes de host.

Antes de criar uma tarefa de restauração para o Db2, assegure-se de que os requisitos a seguir tenham sido atendidos:

- Pelo menos uma tarefa de backup do Db2 foi configurada e está sendo executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do Db2” na página 144](#).
- Funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está configurando a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#).
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Nota: Quando você estiver restaurando bancos de dados multiparticionados para um local alternativo, assegure-se de que a instância de destino esteja configurada com os mesmos números de partição que a instância original. Todas essas partições devem estar em um único host. Quando você está restaurando dados para uma nova instância que é renomeada, ambas as instâncias necessárias para a operação de restauração devem ser configuradas com o mesmo número de partições.

Antes de iniciar uma operação de restauração para uma instância alternativa, certifique-se de que a estrutura do sistema de arquivos na máquina de origem seja correspondida na máquina de destino. Esta estrutura de sistema de arquivos inclui espaços de tabela, logs on-line e o diretório de banco de dados local. Certifique-se de que volumes dedicados com espaço suficiente sejam alocados para a estrutura do sistema de arquivos. O Db2 deve estar no mesmo nível de versão nos hosts de origem e de destino para todas as operações de restauração e deve existir uma instância com o mesmo nome em cada host. Para obter informações adicionais sobre requisitos de espaço, consulte [Requisitos de espaço para proteção do Db2](#). Para obter informações adicionais sobre pré-requisitos e configuração, consulte [Pré-requisitos para o Db2](#).

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Db2** e clique em **Criar tarefa de restauração**.

O assistente Restauração de captura instantânea é aberto.

2. Opcional: Caso tenha iniciado o assistente de restauração a partir da página **Tarefas e operações**, escolha Db2 como o tipo de origem e clique em **Avançar**.

Dica: Para obter um resumo de suas seleções no assistente de restauração, mova o cursor para o ícone de informações  na área de janela de navegação do assistente.

3. Na página **Seleção de origem**, clique em uma instância do Db2 para mostrar os bancos de dados nessa instância. Escolha um banco de dados clicando no ícone de mais  ao lado do nome do banco de dados. Clique em **Avançar** para continuar.
4. Na página **Captura instantânea de origem**, escolha o tipo de operação de restauração necessário.
 - **On demand: captura instantânea:** cria uma operação de restauração única a partir de uma captura instantânea de banco de dados. A tarefa não é configurada para recorrer.
 - **On demand: momento:** cria uma operação de restauração única a partir de um backup de momento do banco de dados. A tarefa não é configurada para recorrer.
 - **Recorrente:** cria uma tarefa recorrente que é executada de acordo com um planejamento e se repete.

Dica:

Para um **On demand: captura instantânea**, é possível selecionar nenhuma recuperação ou recuperar até o término do backup. Para uma tarefa de restauração **On demand: momento**, é possível selecionar para recuperar até o término dos logs disponíveis ou recuperar até um momento específico.

5. Na mesma página, selecione um **Tipo de local de restauração** da seguinte forma:

Local	Instruções
Site	Selecione esta opção para restaurar dados a partir do site primário ou secundário. O site é a única opção para tarefas de restauração de momento sob demanda.
Transferência de nuvem	Selecione esta opção para restaurar dados do armazenamento em nuvem. Especifique o ponto de restauração a ser usado para a captura instantânea.
Transferência de repositório	Selecione esta opção para restaurar dados de um repositório vSnap. Especifique o ponto de restauração a ser usado para a captura instantânea.
Archive de nuvem	Selecione esta opção para restaurar dados que são arquivados na nuvem. Especifique o ponto de restauração a ser usado para a captura instantânea.
Archive de repositório	Selecione esta opção para restaurar dados que estão arquivados no repositório do vSnap. Especifique o ponto de restauração a ser usado para a captura instantânea.

Quando estiver criando uma captura instantânea on demand, é possível especificar um período de tempo na captura instantânea que você está procurando. Quando aplicável, é possível usar um servidor vSnap diferente para a operação.

6. Selecione um local para a operação de restauração. Escolha uma das opções de local a seguir e clique em **Avançar**.

Opção	Descrição
Demo	Selecione esta opção para restaurar dados do servidor vSnap de demonstração. Esta opção está disponível apenas em determinadas configurações.
Primário	Selecione essa opção para restaurar dados do servidor vSnap primário para o destino. Esse local está disponível para o tipo de local de restauração Site.
Secundário	Selecione essa opção para restaurar dados do servidor vSnap secundário para o destino. Esse local está disponível para o tipo de local de restauração Site.

Os pontos de restauração estão disponíveis no menu **Ponto de restauração**.

7. Escolha um **método de restauração** apropriado para o destino escolhido para a operação de restauração. Clique em **Avançar** para continuar.

- **Acesso instantâneo:** Nesse modo, nenhuma ação adicional é executada após o IBM Spectrum Protect Plus montar o volume a partir do repositório do vSnap. Use os dados para recuperação customizada a partir dos arquivos no volume montado.
- **Produção:** Nesse modo, o servidor de aplicativos Db2 primeiro copia os arquivos do volume do repositório do vSnap para o host de destino, que é um local alternativo ou a instância original. Esses dados copiados são então usados para iniciar o banco de dados.
- **Teste:** Nesse modo, o agente cria um novo banco de dados usando os arquivos de dados diretamente do repositório do vSnap.
- Inclua um nome de banco de dados quando estiver restaurando o banco de dados para um local diferente e desejar renomear o banco de dados.

Dica:

A produção é o único **método de restauração** que está disponível para operações de restauração para o local original. Quaisquer opções não apropriadas para a operação de restauração que você selecionou não são selecionáveis.

Para restaurar dados para a instância original, siga as instruções em [Restaurando para a instância original](#). Para restaurar dados para uma instância alternativa, siga as instruções em [Restaurando para uma instância alternativa](#).

8. Configure o destino para a operação de restauração escolhendo uma das opções a seguir. Clique em **Avançar** para continuar.

- **Restaurar para a instância original:** esta opção restaura dados para o servidor original e a instância original.
- **Restaurar para uma instância alternativa:** esta opção restaura os dados para um local especificado diferente, criando uma cópia dos dados nesse local.

Se você estiver restaurando dados para um local alternativo, escolha uma instância na tabela **Instância** antes de clicar em **Avançar**. A instância alternativa deve estar em uma máquina diferente e instâncias inadequadas não estão disponíveis para seleção. Para bancos de dados com multipartição, a instância de destino deve ter o mesmo conjunto de partições em uma única máquina.

9. Na página **Opções da tarefa**, selecione as opções de recuperação, de aplicativo e opções avançadas para a operação de restauração que está sendo definida.

Dica:

As opções de recuperação não estão disponíveis para tarefas de restauração de acesso instantâneo.

- **Sem Recuperação** . Esta opção ignora todo o Rollforward de recuperação após a operação de restauração. O banco de dados permanece em um estado Rollforward pending até que você decida se deseja executar a operação de Rollforward manualmente.
- **Recuperar até o término do backup** . Esta opção recupera o banco de dados selecionado para seu estado no momento em que o backup foi criado. O processo de recuperação usa os arquivos de log que estão incluídos no backup de banco de dados do Db2.
- **Recuperar até o encerramento de logs disponíveis** . Essa opção estará disponível somente se os logs forem submetidos a backup na definição de tarefa de backup do Db2. O IBM Spectrum Protect Plus usa o ponto de restauração mais recente. Um ponto de restauração temporário para backups de log é criado automaticamente para que possa ser executado rollforward do banco de dados Db2 até o encerramento dos logs. Essa opção de recuperação não estará disponível se você tiver selecionado um ponto de restauração específico na lista. Esta opção está disponível somente quando você está executando uma tarefa de restauração momentânea on demand que usa o backup mais recente.
- **Recuperar até um ponto específico-no-tempo** . Essa opção inclui todos os dados de backup até um momento específico. Esta opção estará disponível apenas se você tiver ativado backups de log em sua definição de tarefa de backup do Db2. Configure uma recuperação de momento por uma data e hora específicas, por exemplo, Jan 1, 2019 12:18:00 AM. O IBM Spectrum Protect Plus localiza os pontos de restauração diretamente antes e depois do momento selecionado. Durante o processo de recuperação, são montados o volume de backup de dados mais antigo e o volume de backup de log mais recente. Se o momento for após o último backup, um ponto de restauração temporário será criado. Essa opção de recuperação não estará disponível se você tiver selecionado um ponto de restauração específico na lista. Essa opção está disponível somente quando você está executando uma tarefa de restauração de momento sob demanda que usa o backup mais recente.

Dica: Para ignorar as etapas opcionais no assistente de restauração, selecione **Ignorar etapas opcionais** e clique em **Avançar**.

10. Opcional: Na página **Opções da tarefa**, selecione as opções de aplicativo para a operação de restauração que você está definindo.

Dica:

As opções do aplicativo não estão disponíveis para tarefas de restauração de acesso instantâneo.

- **Sobrescrever bancos de dados existentes** . Escolha esta opção para substituir os bancos de dados existentes que têm os mesmos nomes durante o processo de recuperação de restauração. Se essa opção não estiver selecionada, a tarefa de restauração falhará quando os bancos de dados com o mesmo nome forem localizados durante a operação de restauração. Se você selecionar esta opção, certifique-se de que o diretório de log do Db2 e o diretório de log de espelho do Db2 não tenham dados.



Atenção: Certifique-se de que nenhum outro banco de dados compartilhe o diretório de banco de dados local como o banco de dados original ou esses dados serão sobrescritos quando esta opção for selecionada.

- **Máximo de Fluxos Paralelo por Banco de Dados** . É possível optar por executar a operação de restauração de dados em fluxos paralelos. Essa opção será útil se você estiver restaurando um banco de dados grande.
- **Especifique o tamanho do conjunto de memórias do banco de dados Db2 em KB**. Especifique a memória, em KB, a ser alocada para a restauração do banco de dados na máquina de destino. Este valor é usado para modificar o tamanho de memória compartilhada do banco de dados Db2 no servidor de destino. Para usar o mesmo tamanho de memória compartilhada no servidor de origem e no servidor de destino, configure o valor como zero.

11. Opcional: Na página **Opções da tarefa**, selecione as opções avançadas para a operação de restauração que você está definindo.

- **Executar limpeza imediatamente na falha da tarefa** . Esta opção é selecionada por padrão para limpar automaticamente os recursos alocados como parte de uma operação de restauração quando a recuperação falha.
 - **Continuar com restaurações de outros bancos de dados selecionados mesmo que um falhe**. Esta opção continuará a operação de restauração se um banco de dados na instância não for restaurado com sucesso. O processo continua para todos os outros bancos de dados que estão sendo restaurados. Quando esta opção não estiver selecionada, a tarefa de restauração será parada quando a recuperação de um recurso falhar.
 - **Prioridade de protocolo**: Durante uma tarefa de restauração de **Acesso instantâneo**, escolha entre **iSCSI** e **Fibre Channel** como o protocolo de prioridade a ser usado para a tarefa de restauração.
 - **Prefixo do ponto de montagem**. Para operações de restauração de acesso instantâneo, especifique o prefixo para o caminho para onde o ponto de montagem será direcionado.
12. Escolha as opções de script na página **Aplicar scripts** e clique em **Avançar** para continuar.
- Selecione **Pré-Script** para selecionar um script transferido por upload e um servidor de aplicativos ou de script em que o pré-script é executado. Para selecionar um servidor de aplicativos no qual o script é executado, desmarque a caixa de seleção **Usar servidor de script**. Acesse a página **Configuração do sistema > Script** para configurar scripts e servidores de script.
 - Selecione **Pós-script** para selecionar um script transferido por upload e um servidor de aplicativos ou de script em que o pós-script é executado. Para selecionar um servidor de aplicativos no qual o script é executado, desmarque a caixa de seleção **Usar servidor de script**. Acesse a página **Configuração do sistema > Script** para configurar scripts e servidores de script.
 - Selecione **Continuar a tarefa durante erro do script** para continuar executando a tarefa quando o script que está associado à tarefa falhar. Quando esta opção estiver ativada e o pré-script for concluído com um código de retorno diferente de zero, a tarefa de backup ou de restauração continuará sendo executada e o status da tarefa de pré-script retornará COMPLETED. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa de pós-script retornará COMPLETED. Quando esta opção não estiver selecionada, a tarefa de backup ou de restauração não será executada, e o status da tarefa de pré-script ou pós-script será retornado com um status FAILED.
13. Na página **Planejamento** , nomeie a tarefa de restauração e escolha a frequência para a execução da tarefa. Planeje o horário de início e clique em **Avançar** para continuar.
- Caso a tarefa de restauração que está sendo especificada seja uma tarefa on demand, não há opção para inserir um planejamento. Especifique um planejamento apenas para tarefas de restauração contínuas.
14. Na página **Revisar**, revise suas seleções para a tarefa de restauração. Se todos os detalhes estiverem corretos para sua tarefa de restauração, clique em **Enviar** ou clique em **Voltar** para fazer as mudanças.

Resultados

Poucos minutos depois de clicar em **Enviar**, o registro **onDemandRestore** é incluído na área de janela **Sessões da tarefa**. Para visualizar o progresso da operação de restauração, expanda a tarefa. Também é possível fazer download do arquivo de log clicando no ícone de download  . Todas as tarefas em execução são visualizáveis na página **Tarefas e operações** **Tarefas em execução**.

Para restaurar dados para a instância original, siga as instruções em [Restaurando para a instância original](#). Para restaurar dados para uma instância alternativa, siga as instruções em [Restaurando para uma instância alternativa](#).

Restaurando dados do Db2 para a instância original

É possível restaurar um backup de banco de dados para sua instância original no host original. É possível restaurar para o backup mais recente ou para uma versão de backup de banco de dados anterior do Db2. Ao restaurar um banco de dados para sua instância original, não é possível renomeá-lo. Essa opção de

restauração executa uma restauração completa da produção de dados, e os dados existentes serão sobrescritos no site de destino se a opção **Sobrescrever bancos de dados existentes** estiver selecionada.

Antes de Iniciar

Se o seu ambiente Db2 incluir bancos de dados particionados, os dados de todas as partições serão submetidos a backup durante tarefas de backup regulares. Todas as instâncias são listadas na área de janela de backup. As instâncias multiparticionadas são mostradas com números de partição e nomes de host.

Antes de criar uma tarefa de restauração para o Db2, assegure-se de que os requisitos a seguir tenham sido atendidos:

- Pelo menos uma tarefa de backup do Db2 foi configurada e está sendo executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do Db2”](#) na página 144.
- Funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está configurando a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297.
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Db2** e clique em **Criar tarefa de restauração**.

O assistente Restauração de captura instantânea é aberto.

2. Opcional: Caso tenha iniciado o assistente de restauração a partir da página **Tarefas e operações**, escolha Db2 como o tipo de origem e clique em **Avançar**.

Dica: Para obter um resumo de suas seleções no assistente de restauração, mova o cursor para o ícone de informações  na área de janela de navegação do assistente.

3. Na página **Seleção de origem**, clique em uma instância do Db2 para mostrar os bancos de dados nessa instância. Escolha um banco de dados clicando no ícone de mais  ao lado do nome do banco de dados. Clique em **Avançar** para continuar.

4. Na página **Captura instantânea de origem**, escolha o tipo de operação de restauração necessário.

- **On demand: captura instantânea:** cria uma operação de restauração única a partir de uma captura instantânea de banco de dados. A tarefa não é configurada para recorrer.
- **On demand: momento:** cria uma operação de restauração única a partir de um backup de momento do banco de dados. A tarefa não é configurada para recorrer.
- **Recorrente:** cria uma tarefa recorrente que é executada de acordo com um planejamento e se repete.

Dica:

Para um **On demand: captura instantânea**, é possível selecionar nenhuma recuperação ou recuperar até o término do backup. Para uma tarefa de restauração **On demand: momento**, é possível selecionar para recuperar até o término dos logs disponíveis ou recuperar até um momento específico.

5. Na mesma página, selecione um **Tipo de local de restauração** da seguinte forma:

Local	Instruções
Site	Selecione esta opção para restaurar dados a partir do site primário ou secundário. O site é a

Local	Instruções
	única opção para tarefas de restauração de momento sob demanda.
Transferência de nuvem	Selecione esta opção para restaurar dados do armazenamento em nuvem. Especifique o ponto de restauração a ser usado para a captura instantânea.
Transferência de repositório	Selecione esta opção para restaurar dados de um repositório vSnap. Especifique o ponto de restauração a ser usado para a captura instantânea.
Archive de nuvem	Selecione esta opção para restaurar dados que são arquivados na nuvem. Especifique o ponto de restauração a ser usado para a captura instantânea.
Archive de repositório	Selecione esta opção para restaurar dados que estão arquivados no repositório do vSnap. Especifique o ponto de restauração a ser usado para a captura instantânea.

Quando estiver criando uma captura instantânea on demand, é possível especificar um período de tempo na captura instantânea que você está procurando. Quando aplicável, é possível usar um servidor vSnap diferente para a operação.

- Selecione um local para a operação de restauração. Escolha uma das opções de local a seguir e clique em **Avançar**.

Opção	Descrição
Demo	Selecione esta opção para restaurar dados do servidor vSnap de demonstração. Esta opção está disponível apenas em determinadas configurações.
Primário	Selecione essa opção para restaurar dados do servidor vSnap primário para o destino. Esse local está disponível para o tipo de local de restauração Site.
Secundário	Selecione essa opção para restaurar dados do servidor vSnap secundário para o destino. Esse local está disponível para o tipo de local de restauração Site.

Os pontos de restauração estão disponíveis no menu **Ponto de restauração**.

- Na página **Método de restauração**, escolha **Produção** para a operação de restauração.

No modo de **Produção**, o servidor de aplicativos Db2 primeiro copia os arquivos do volume de repositório vSnap para o host de destino. Esses dados copiados são então usados para iniciar o banco de dados.

Dica: Evite inserir um novo nome de banco de dados quando você estiver restaurando uma operação de produção para a instância original, uma vez que ela não será implementada.

- Configure o destino para a operação de restauração para **Restaurar para a instância original** para restaurar dados para o servidor original. Clique em **Avançar** para continuar.
- Escolha as opções, conforme descrito em [“Restaurando Dados do Db2”](#) na página 151.

10. Na página **Planejamento**, nomeie a tarefa de restauração e escolha a frequência para a execução da tarefa. Planeje o horário de início e clique em **Avançar** para continuar.

Caso a tarefa de restauração que está sendo especificada seja uma tarefa on demand, não há opção para inserir um planejamento. Especifique um planejamento apenas para tarefas de restauração contínuas.

11. Na página **Revisar**, revise suas seleções para a tarefa de restauração. Se todos os detalhes estiverem corretos para sua tarefa de restauração, clique em **Enviar** ou clique em **Voltar** para fazer as mudanças.

Resultados

Poucos minutos depois de clicar em **Enviar**, o registro **onDemandRestore** é incluído na área de janela **Sessões da tarefa**. Para visualizar o progresso da operação de restauração, expanda a tarefa. Também é

possível fazer download do arquivo de log clicando no ícone de download . Todas as tarefas em execução são visualizáveis na página **Tarefas e operações Tarefas em execução**.

Restaurando bancos de dados do Db2 para uma instância alternativa

É possível restaurar um banco de dados Db2 para outra instância do Db2 em um host alternativo. Também é possível optar por restaurar um banco de dados para uma instância com um nome diferente e renomear o banco de dados. Este processo cria uma cópia exata do banco de dados em um host diferente em uma instância diferente. Se estiver restaurando um recurso para um local alternativo, é possível restaurar o mesmo recurso várias vezes sem especificar hosts de destino diferentes.

Antes de Iniciar

Importante: Para todas as operações de restauração, o Db2 deve estar no mesmo nível de versão nos hosts de origem e de destino. Além desse requisito, deve-se assegurar que uma instância com o mesmo nome que a instância que está sendo restaurada exista em cada host. Esse requisito se aplica quando a instância de destino tem o mesmo nome e quando os nomes são diferentes. Para que a operação de restauração seja bem-sucedida, ambas as instâncias devem ser provisionadas, uma com o nome original e a outra com o novo nome.

Antes de criar uma tarefa de restauração para o Db2, assegure-se de que os requisitos a seguir tenham sido atendidos:

- Pelo menos uma tarefa de backup do Db2 foi configurada e está sendo executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do Db2” na página 144](#).
- Funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está configurando a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#).
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Antes de iniciar uma operação de restauração para uma instância alternativa, certifique-se de que a estrutura do sistema de arquivos na máquina de origem seja correspondida na máquina de destino. Esta estrutura de sistema de arquivos inclui espaços de tabela, logs on-line e o diretório de banco de dados local. Certifique-se de que volumes dedicados com espaço suficiente sejam alocados para a estrutura do sistema de arquivos. O Db2 deve estar no mesmo nível de versão nos hosts de origem e de destino para todas as operações de restauração e deve existir uma instância com o mesmo nome em cada host. Para obter informações adicionais sobre requisitos de espaço, consulte [Requisitos de espaço para proteção do Db2](#). Para obter informações adicionais sobre pré-requisitos e configuração, consulte [Pré-requisitos para o Db2](#).

Restrição: Se existirem dados no diretório de banco de dados local para o qual você está restaurando o backup de banco de dados e a opção **Sobrescrever bancos de dados existentes** não estiver selecionada, a operação de restauração falhará. Nenhum outro dado pode compartilhar o diretório do banco de dados

local no qual o backup é restaurado. Quando a opção **Sobrescrever bancos de dados existentes** é selecionada, todos os dados existentes são removidos, além do diretório do banco de dados local no host alternativo.

Nota: Quando você estiver restaurando bancos de dados multiparticionados para um local alternativo, assegure-se de que a instância de destino esteja configurada com os mesmos números de partição que a instância original. Todas essas partições devem estar em um único host. Quando você está restaurando dados para uma nova instância que é renomeada, ambas as instâncias necessárias para a operação de restauração devem ser configuradas com o mesmo número de partições.

Sobre Esta Tarefa

Certifique-se de que os caminhos do disco para a operação de restauração direcionada incluam o nome da instância e o nome do banco de dados. As informações são necessárias para todos os tipos de caminhos: caminhos do banco de dados, caminhos do contêiner, caminhos de armazenamento e caminhos de log e de log de espelho.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Db2** e clique em **Criar tarefa de restauração**.

O assistente Restauração de captura instantânea é aberto.

2. Opcional: Caso tenha iniciado o assistente de restauração a partir da página **Tarefas e operações**, escolha Db2 como o tipo de origem e clique em **Avançar**.

Dica: Para obter um resumo de suas seleções no assistente de restauração, mova o cursor para o ícone de informações  na área de janela de navegação do assistente.

3. Na página **Seleção de origem**, clique em uma instância do Db2 para mostrar os bancos de dados nessa instância. Escolha um banco de dados clicando no ícone de mais  ao lado do nome do banco de dados. Clique em **Avançar** para continuar.

4. Na página **Captura instantânea de origem**, escolha o tipo de operação de restauração necessário.

- **On demand: captura instantânea:** cria uma operação de restauração única a partir de uma captura instantânea de banco de dados. A tarefa não é configurada para recorrer.
- **On demand: momento:** cria uma operação de restauração única a partir de um backup de momento do banco de dados. A tarefa não é configurada para recorrer.
- **Recorrente:** cria uma tarefa recorrente que é executada de acordo com um planejamento e se repete.

Dica:

Para um **On demand: captura instantânea**, é possível selecionar nenhuma recuperação ou recuperar até o término do backup. Para uma tarefa de restauração **On demand: momento**, é possível selecionar para recuperar até o término dos logs disponíveis ou recuperar até um momento específico.

5. Na mesma página, selecione um **Tipo de local de restauração** da seguinte forma:

Local	Instruções
Site	Selecione esta opção para restaurar dados a partir do site primário ou secundário. O site é a única opção para tarefas de restauração de momento sob demanda.
Transferência de nuvem	Selecione esta opção para restaurar dados do armazenamento em nuvem. Especifique o ponto de restauração a ser usado para a captura instantânea.

Local	Instruções
Transferência de repositório	Selecione esta opção para restaurar dados de um repositório vSnap. Especifique o ponto de restauração a ser usado para a captura instantânea.
Archive de nuvem	Selecione esta opção para restaurar dados que são arquivados na nuvem. Especifique o ponto de restauração a ser usado para a captura instantânea.
Archive de repositório	Selecione esta opção para restaurar dados que estão arquivados no repositório do vSnap. Especifique o ponto de restauração a ser usado para a captura instantânea.

Quando estiver criando uma captura instantânea on demand, é possível especificar um período de tempo na captura instantânea que você está procurando. Quando aplicável, é possível usar um servidor vSnap diferente para a operação.

- Selecione um local para a operação de restauração. Escolha uma das opções de local a seguir e clique em **Avançar**.

Opção	Descrição
Demo	Selecione esta opção para restaurar dados do servidor vSnap de demonstração. Esta opção está disponível apenas em determinadas configurações.
Primário	Selecione essa opção para restaurar dados do servidor vSnap primário para o destino. Esse local está disponível para o tipo de local de restauração Site.
Secundário	Selecione essa opção para restaurar dados do servidor vSnap secundário para o destino. Esse local está disponível para o tipo de local de restauração Site.

Os pontos de restauração estão disponíveis no menu **Ponto de restauração**.

- Escolha um **método de restauração** apropriado para o destino escolhido para a operação de restauração. Clique em **Avançar** para continuar.
 - Produção:** Nesse modo, o servidor de aplicativos Db2 primeiro copia os arquivos do volume do repositório do vSnap para o host de destino, que é um local alternativo ou a instância original. Esses dados copiados são então usados para iniciar o banco de dados.
 - Teste:** Nesse modo, o agente cria um novo banco de dados usando os arquivos de dados diretamente do repositório do vSnap.
 - Acesso instantâneo:** Nesse modo, nenhuma ação adicional é executada após o IBM Spectrum Protect Plus montar o volume a partir do repositório do vSnap. Use os dados para recuperação customizada a partir dos arquivos no volume montado.
 - Inclua um nome de banco de dados quando estiver restaurando o banco de dados para um local diferente e desejar renomear o banco de dados.
- Configure o destino para a operação de restauração como **Restaurar para uma instância alternativa** para restaurar dados para um local diferente, que pode ser selecionado na lista de locais elegíveis. Clique em **Avançar** para continuar.

Quando você estiver restaurando para um local alternativo, escolha uma instância na tabela **Instância** antes de clicar em **Avançar**. As instâncias de destino inadequadas não podem ser selecionadas.

9. Escolha as opções, conforme descrito em “Restaurando Dados do Db2 ” na página 151.
10. Na página **Planejamento** , nomeie a tarefa de restauração e escolha a frequência para a execução da tarefa. Planeje o horário de início e clique em **Avançar** para continuar.

Caso a tarefa de restauração que está sendo especificada seja uma tarefa on demand, não há opção para inserir um planejamento. Especifique um planejamento apenas para tarefas de restauração contínuas.
11. Na página **Revisar**, revise suas seleções para a tarefa de restauração. Se todos os detalhes estiverem corretos para sua tarefa de restauração, clique em **Enviar** ou clique em **Voltar** para fazer as mudanças.

Resultados

Poucos minutos depois de clicar em **Enviar**, o registro **onDemandRestore** é incluído na área de janela **Sessões da tarefa**. Para visualizar o progresso da operação de restauração, expanda a tarefa. Também é possível fazer download do arquivo de log clicando no ícone de download  . Todas as tarefas em execução são visualizáveis na página **Tarefas e operações Tarefas em execução**.

Microsoft Exchange Servidor

Depois de registrar com sucesso um Microsoft Exchange Server, é possível começar a proteger dados do Microsoft Exchange com o IBM Spectrum Protect Plus. Defina uma política de acordo de nível de serviço (ANS) para criar tarefas de backup com planejamentos específicos, políticas de retenção e scripts.

Pré-requisitos para o Servidor Microsoft Exchange

Certifique-se de que todos os pré-requisitos para o aplicativo Microsoft Exchange sejam atendidos antes de você começar a proteger bancos de dados Microsoft Exchange com o IBM Spectrum Protect Plus.

Para obter mais informações, consulte “Microsoft Requisitos do Exchange Server” na página 28.

Suporte de virtualização

O IBM Spectrum Protect Plus suporta o Microsoft Exchange Server em execução em um servidor físico (bare metal), bem como um ambiente de virtualização. Os ambientes de virtualização a seguir são suportados:

- Sistema operacional guest do VMware ESX
- Microsoft Windows Hyper-V guest sistema operacional

Privilégios

Para ajudar a assegurar que um agente do Microsoft Exchange possa funcionar no ambiente IBM Spectrum Protect Plus, deve-se configurar privilégios apropriados.

Controle de Acesso Baseado na Função

Para segurança do IBM Spectrum Protect Plus, os usuários que estão com logon efetuado no Exchange Server devem ter permissões de controle de acesso baseado na função (RBAC) para acessar caixas de correio e para concluir tarefas de restauração de caixa de correio.

Você deve designar as funções de gerenciamento a seguir a cada usuário do Exchange que executará tarefas de restauração de caixa de correio:

- Permissões do Active Directory
- ApplicationImpersonation

- Bancos de dados
- Recuperação de Desastres
- Exportação e importação da caixa de correio
- Pastas públicas
- Configuração somente visualização
- Destinatários somente visualização

Recomendamos que os usuários que você deseja que executem tarefas de restauração da caixa de correio sejam colocados em um grupo de funções do Exchange Server que contém as funções acima.

O Exchange Server inclui vários grupos de funções integrados. Por padrão, o grupo de funções Gerenciamento da organização conterá a maioria, se não todas, as funções listadas acima.

Recomendamos que o usuário que você deseja que execute tarefas de restauração da caixa de correio seja colocado no grupo de funções Gerenciamento da organização (assegurando que ele contenha todas as funções listadas acima).

Alternativamente, é possível colocar o usuário em outro grupo de funções criado ou em qualquer outro grupo de funções integrado que contenha as funções listadas acima.

Nota: Um usuário cujo nome não está no grupo ou subgrupos de funções de Gerenciamento da Organização do Exchange pode ter um desempenho mais lento ao concluir operações de restauração.

Nota: Você poderá gerenciar grupos de funções do Exchange usando o Exchange Admin Center (EAC) ou Cmdlets do Exchange Powershell **apenas** se seu nome de usuário estiver autorizado pela política de segurança em sua organização.

Escopo da função de gerenciamento

Certifique-se de que os seguintes objetos do Exchange estejam no escopo da função de gerenciamento para o usuário do Exchange:

- O Exchange Server que contém os dados necessários.
- O banco de dados de recuperação que é criado por IBM Spectrum Protect Plus.
- O banco de dados que contém a caixa de correio ativa.
- O banco de dados que contém a caixa de correio ativa do usuário que conclui a operação de restauração.

Verifique se o nome do usuário do Exchange é membro de um grupo de Administradores locais e possui uma caixa de correio ativa do Exchange no domínio. Por padrão, o Windows inclui o grupo de Administradores da Organização do Exchange em outros grupos de segurança, incluindo o grupo de Administradores locais. Para usuários do Exchange que não são membros do grupo de Gerenciamento da Organização do Exchange, deve-se incluir manualmente a conta do usuário no grupo de Administradores locais usando a ferramenta Usuários e grupos locais no computador do membro de domínio.

No computador do membro de domínio, clique em **Ferramentas administrativas > Gerenciamento de computadores > Ferramenta Usuários e grupos locais**. Em um computador do controlador de domínio que não tenha um grupo de Administradores locais ou uma ferramenta Usuários e grupos locais, inclua manualmente a conta do usuário no grupo de Administradores no domínio, clicando em **Ferramentas administrativas > Ferramenta Usuários e computadores do Active Directory**.

Criptografando Sistema de Arquivos

O IBM Spectrum Protect Plus para Exchange requer que o Sistema de Arquivos com Criptografia (EFS) esteja ativado na política de domínio local ou de grupo, e um certificado válido de Domain Data Recovery Agent (DRA) está disponível. Se uma política de grupo customizado estiver definida e vinculada à unidade organizacional, certifique-se de que o servidor Exchange seja parte da unidade organizacional.

Incluindo um Microsoft Exchange servidor de aplicativos

Ao registrar o Microsoft Exchange Server, um inventário de bancos de dados do Exchange é incluído no IBM Spectrum Protect Plus. Quando o inventário estiver disponível, é possível iniciar o backup e a restauração de bancos de dados do Exchange e executar relatórios.

Sobre Esta Tarefa

Para registrar um servidor de aplicativos Microsoft Exchange, é necessário o endereço IP ou o nome do host.

Procedimento

Para incluir um servidor de aplicativos Microsoft Exchange, conclua as seguintes etapas:

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Exchange**.
2. Na página **Exchange**, clique em **Gerenciar servidores de aplicativos** e, em seguida, clique em **Incluir servidor de aplicativos** para incluir o sistema host.
3. No formulário **Propriedades do aplicativo**, insira o endereço IP ou do host.
4. Insira um ID do usuário no formato de domínio e de conta do usuário do Active Directory (domain \user) e a senha associada. Este usuário deve ter as funções e privilégios corretos do Exchange. Para obter informações adicionais sobre privilégios do Exchange, consulte [“Privilégios”](#) na página 161.
5. Clique em **Salvar** e repita as etapas para incluir outras instâncias do Microsoft Exchange no IBM Spectrum Protect Plus.

Importante: Em um ambiente do grupo de disponibilidade do banco de dados (DAG), registre todos os servidores de aplicativos Microsoft Exchange no DAG.

O que Fazer Depois

Ao incluir o servidor de aplicativos Exchange no IBM Spectrum Protect Plus, um inventário é executado automaticamente em cada instância. Os bancos de dados devem ser detectados para assegurar que eles possam ser submetidos a backup e é possível executar um inventário manual a qualquer momento para detectar atualizações. Para obter instruções sobre como executar um inventário manual, consulte [“Detectando Microsoft Exchange bancos de dados executando um inventário”](#) na página 163. Para obter instruções sobre como configurar tarefas de backup do banco de dados do Exchange, consulte [“Definindo uma tarefa de backup de Acordo de Nível de Serviço”](#) na página 165.

Detectando Microsoft Exchange bancos de dados executando um inventário

Ao incluir suas instâncias do Microsoft Exchange Server no IBM Spectrum Protect Plus, um inventário é executado automaticamente. No entanto, é possível executar manualmente um inventário em um servidor de aplicativos Exchange a qualquer momento para detectar atualizações e listar todos os bancos de dados do Exchange para cada instância.

Antes de Iniciar

Certifique-se de que tenha incluído instâncias do Exchange no IBM Spectrum Protect Plus. Para obter instruções sobre como incluir uma instância do Exchange, consulte [“Incluindo um Microsoft Exchange servidor de aplicativos”](#) na página 163.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Exchange**.
2. Clique em **Executar inventário**.
Quando o inventário está em execução, o rótulo do botão muda para **Inventário em andamento**. É possível executar um inventário em qualquer servidor de aplicativos disponível, mas é possível executar apenas um processo de inventário de cada vez.
3. Para monitorar a tarefa de inventário, acesse **Tarefas e operações**. Clique na guia **Tarefas em execução** e procure a entrada do log Inventário do servidor de aplicativos mais recente.

As tarefas concluídas são mostradas na guia **Histórico da tarefa**. É possível usar a lista **Classificar por** para classificar tarefas com base no horário de início, no tipo, no status, no nome ou na duração da tarefa. Use o campo **Procurar por nome** para procurar tarefas por nome. É possível utilizar asteriscos como caracteres curinga no nome.

4. Quando a tarefa de inventário estiver concluída, na área de janela **Backup do Exchange**, clique em uma instância do Exchange para abrir uma visualização que mostra os bancos de dados que são detectados para essa instância. Se algum banco de dados estiver ausente na lista **Instâncias**, verifique seu servidor de aplicativos Microsoft Exchange e execute novamente o inventário.

Dica: Para retornar à lista de instâncias, clique no hipertexto **Instâncias** na área de janela Backup do Exchange.

Testando a conexão Microsoft Exchange

Depois de registrar um servidor de aplicativos Microsoft Exchange e de incluí-lo na lista de servidores de aplicativos, teste a conexão. O teste verifica a comunicação entre o IBM Spectrum Protect Plus e o servidor de aplicativos do host.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Exchange**.
2. Na página **Exchange**, clique em **Gerenciar servidores de aplicativos**.
Os servidores de aplicativos Microsoft Exchange que estão disponíveis são mostrados.
3. Clique em **Ações** para o servidor de aplicativos Microsoft Exchange que você deseja testar e, em seguida, clique em **Testar**.

O relatório de teste mostra uma lista dos testes que foram executados e seus status. Cada procedimento de teste inclui um teste da configuração de rede do host físico, um teste de sessão remota e os pré-requisitos de um teste do Windows, como privilégios de administrador de usuário.

4. Clique em **OK** para fechar o teste. Execute o teste novamente depois de corrigir quaisquer problemas.

Fazendo backup de bancos de dados Microsoft Exchange

Para proteger bancos de dados Microsoft Exchange, é possível definir uma tarefa de backup que é executada continuamente para criar backups incrementais. Também é possível executar tarefas de backup on-demand fora do planejamento.

Antes de Iniciar

Certifique-se de que os servidores de aplicativos que contêm os bancos de dados do Exchange dos quais você deseja fazer backup sejam incluídos. Para obter mais informações, consulte [“Incluindo um Microsoft Exchange servidor de aplicativos”](#) na página 163.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Exchange**.
2. Na área de janela **Backup do Exchange**, clique na instância do Microsoft Exchange e, em seguida, selecione o banco de dados para fazer backup.

Cada banco de dados é listado por nome de instância ou de banco de dados, pela política de SLA aplicada e pela elegibilidade para o backup de log.

3. Clique em **Executar**.

A tarefa de backup é iniciada e é possível visualizar os detalhes em **Tarefas e Operação > Tarefas em execução**.

Dica: O botão **Executar** é ativado somente para um backup de banco de dados único e o banco de dados deve ter uma política SLA aplicada.

4. Para executar tarefas de backup para diversos bancos de dados, selecione os bancos de dados na área de janela de backup do Exchange e clique em **Selecionar uma política de SLA**.

Para obter mais informações sobre a definição de tarefas de backup e de opções de tarefa de backup de política de SLA, consulte [“Definindo uma tarefa de backup de Acordo de Nível de Serviço”](#) na página 165.

Definindo uma tarefa de backup de Acordo de Nível de Serviço

Quando seus bancos de dados Microsoft Exchange estiverem listados para cada uma das instâncias do Exchange, selecione e aplique uma política de acordo de nível de serviço (ANS) para começar a proteger seus dados.

Sobre Esta Tarefa

O IBM Spectrum Protect Plus suporta bancos de dados Microsoft Exchange únicos ou múltiplos por tarefa de backup do Exchange. Várias tarefas de backup de banco de dados são executadas sequencialmente.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Exchange**.
2. Selecione uma instância do Exchange para fazer backup de todos os dados nessa instância, ou clique em um nome de instância e, em seguida, selecione bancos de dados individuais dos quais você deseja fazer backup.
3. Clique em **Selecionar uma política de SLA** e escolha uma Política de SLA.
As opções predefinidas são Ouro, Prata e Bronze, cada uma com diferentes frequências e taxas de retenção. Ouro é o mais frequente com a menor taxa de retenção. Também é possível criar uma política de ANS customizada ou editar uma política existente. Para obter mais informações, consulte [“Criando uma política de SLA”](#) na página 89.
4. Clique em **Selecionar opções** para definir opções para seu backup, como ativar backups de log para futuras opções de recuperação e especificar os fluxos paralelos para reduzir o tempo gasto para fazer backup de bancos de dados grandes. Salve suas mudanças.
5. Configure a política de ANS clicando no ícone na coluna **Opções de política** da tabela **Status de política de ANS**.
Para obter informações adicionais sobre opções de configuração de ANS, consulte [“Configurando opções de configuração de ANS para uma tarefa de backup”](#) na página 165.
6. Para executar a política fora da tarefa planejada, selecione a instância ou banco de dados e, em seguida, clique em **Ações > Iniciar**.
O status muda para **Em execução** para seu ANS escolhido. Para pausar o planejamento, clique em **Actions > Pausar planejamento** e para cancelar uma tarefa após ela ter sido iniciada, clique em **Ações > Cancelar**.

Configurando opções de configuração de ANS para uma tarefa de backup

Depois de configurar um acordo de nível de serviço, (ANS), para sua tarefa de backup, é possível optar por configurar mais opções para essa tarefa. As opções extras de ANS incluem executar scripts, excluir recursos da operação de backup e forçar uma cópia de backup de base completo, se necessário.

Procedimento

1. Na coluna **Opções de política** da tabela **Status da política de ANS** para a tarefa que está sendo configurada, clique no ícone da área de transferência para especificar opções de configuração adicionais.
2. Para definir uma configuração de pré-script, selecione **Pré-script** e execute uma das seguintes ações:
 - Para usar um servidor de script, selecione **Usar servidor de script** e escolha um script transferido por upload da lista **Script** ou **Servidor de script**.
 - Para executar um script em um servidor de aplicativos, desmarque a caixa de seleção **Usar servidor de script** e escolha um servidor de aplicativos da lista **Servidor de aplicativos**.
3. Para definir uma configuração de pós-script, selecione **Pós-script** execute uma das seguintes ações:

- Para usar um servidor de script, selecione **Usar servidor de script** e escolha um script transferido por upload da lista **Script** ou **Servidor de script**.
- Para executar um script em um servidor de aplicativos, desmarque a caixa de seleção **Usar servidor de script** e escolha um servidor de aplicativos da lista **Servidor de aplicativos**.

Os scripts e servidores de script são configurados na página **Configuração do sistema > Script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#).

4. Selecione **Continuar a tarefa durante erro do script** para continuar executando a tarefa quando o script que está associado à tarefa falhar.

Se essa opção estiver selecionada, a operação de backup ou de restauração será tentada e o status da tarefa de script será relatado como COMPLETED quando o script concluir o processamento com um código de retorno diferente de zero. Se essa opção não estiver selecionada, o backup ou a restauração não será tentada e o status da tarefa de script será relatado como FAILED.

5. Especifique recursos para excluí-los da tarefa de backup. Insira um nome de recurso exato no campo **Excluir recursos**. Se não tiver certeza de um nome, use asteriscos curinga que são especificados antes do padrão (**text*) ou depois do padrão (*text**). Vários curingas podem ser inseridos com caracteres alfanuméricos padrão e os seguintes caracteres especiais: - _ e *. Separe as entradas com um ponto-e-vírgula.
6. Se desejar criar um backup completo de um recurso específico, insira o nome desse recurso no campo **Forçar backup completo de recursos**. Separe vários recursos com um ponto-e-vírgula.
Um backup completo substitui o backup existente desse recurso apenas para uma ocorrência. Depois disso, o recurso é submetido a backup incremental como antes.
7. Clique em **Salvar**.

Fazendo backup de logs do banco de dados Microsoft Exchange

É possível fazer backup dos logs de transações do banco de dados para bancos de dados Microsoft Exchange. Os backups de log do Exchange são planejados usando o Planejador de Tarefas do Windows. Quando os backups de log estão disponíveis, é possível executar uma recuperação de dados de rollforward durante uma operação de restauração para assegurar que os dados sejam recuperados para o momento mais recente possível.

Sobre Esta Tarefa

Quando os backups de log são ativados, uma tarefa do Planejador de Tarefas é criada no servidor Exchange. A tarefa executa uma operação de backup de seus arquivos de log do Exchange de acordo com a política de ANS.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Exchange**.
2. Clique na instância do Microsoft Exchange que deseja proteger e, em seguida, selecione o banco de dados de cujos logs você deseja fazer backup.

Dica: A coluna **Elegível para backup do log** mostra os bancos de dados para os quais é possível executar backups de log. Se um banco de dados estiver registrado como não elegível para o backup do log, uma explicação de ajuda instantânea será fornecida.

3. Clique em **Selecionar opções** e, em seguida, selecione **Ativar backup do log**.
4. Insira a frequência dos backups de log em dias, horas ou minutos.
5. Escolha a data de início e selecione a hora para que os backups de log sejam iniciados e, em seguida, clique em **Salvar**.

Resultados

Os logs de transações do banco de dados são submetidos a backup para o servidor vSnap, de acordo com a frequência selecionada.

Restrição: Os logs do banco de dados são submetidos a backup somente no nó preferencial. Apenas uma instância do Microsoft Exchange de cada vez pode gravar backups de log no servidor vSnap.

Quaisquer problemas de backup de log que ocorrem são exibidos nas notificações de Alerta no IBM Spectrum Protect Plus.

Fazendo backup de bancos de dados Exchange em um Grupo de Disponibilidade do Banco de Dados

É possível fazer backup dos bancos de dados da caixa de correio em um Grupo de Disponibilidade do Banco de Dados (DAG) do Microsoft Exchange e especificar se será usada a cópia ativa ou uma cópia passiva do banco de dados para o backup. Os servidores Exchange em um ambiente DAG sincronizam os dados entre cópias ativas e passivas para alta disponibilidade.

Sobre Esta Tarefa

Usando as informações de uma tarefa de inventário, o IBM Spectrum Protect Plus fornece uma visualização do DAG que exibe todos os bancos de dados em um ambiente DAG do Exchange. Cada banco de dados tem uma cópia ativa em m servidor no DAG, e uma ou mais cópias passivas nos outros servidores. Por padrão, os backups planejados são obtidos do servidor no qual o banco de dados está ativo, mas é possível selecionar um servidor diferente para fazer backup de uma cópia passiva do banco de dados.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Aplicativos > Exchange**.
2. Na área de janela **Backup do Exchange**, clique no menu **Visualizar** e selecione **Grupos de disponibilidade do banco de dados**.
3. Clique no DAG do Microsoft Exchange que você deseja visualizar e, em seguida, selecione os bancos de dados para backup.
4. Clique em **Selecionar Opções**. Na lista **Nó preferencial de backup**, selecione a instância do na qual executar os backups.
Com a opção **Nó preferencial de backup**, é possível selecionar uma cópia passiva do banco de dados para o backup.
5. Clique em **Selecionar uma política de SLA** e, em seguida, selecione uma política de SLA na lista.
6. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.
Os bancos de dados DAG são planejados para tarefas de backup de acordo com as políticas de ANS selecionadas e as opções do nó preferencial.
7. Para executar a política selecionada fora do planejamento, na área de janela **Status da política de ANS**, clique em **Ações > Iniciar**.

Estratégia de Backup Incremental Contínuo

O IBM Spectrum Protect Plus fornece uma estratégia de backup chamada *incremental contínua*. Em vez de planejar tarefas periódicas de backup completo, esta solução de backup requer apenas um backup completo inicial. Posteriormente, ocorre uma sequência contínua de tarefas de backup incremental.

A solução de backup incremental contínuo fornece as seguintes vantagens:

- Reduz a quantidade de dados que passam pela rede
- Reduz o crescimento de dados porque todos os backups incrementais contêm apenas os blocos que mudaram desde o backup anterior
- Reduz a duração de tarefas de backup

O processo incremental contínuo do IBM Spectrum Protect Plus inclui as seguintes etapas:

1. A primeira tarefa de backup cria uma captura instantânea do VSS do aplicativo Exchange. Como resultado, os arquivos de banco de dados estão em um estado consistente do aplicativo. Os arquivos de banco de dados completos são copiados para o local do vSnap.
2. Todos os backups subsequentes criam uma captura instantânea do VSS do aplicativo Exchange. Os arquivos de banco de dados estão em um estado consistente do aplicativo. No entanto, somente os blocos de mudança dos arquivos de banco de dados são copiados para o local do vSnap.

- Os backups são reconstruídos em cada momento em que um backup é executado, tornando possível a recuperação do banco de dados a partir de qualquer ponto de backup único.

Restaurando Microsoft Exchange bancos de dados

Se os dados em um banco de dados Microsoft Exchange não estiverem perdidos ou corrompidos, é possível restaurá-los de uma cópia de backup. Use o assistente "Restauração de Captura Instantânea" para configurar um planejamento de tarefa de restauração ou uma operação de restauração on demand. É possível definir uma tarefa que restaura dados para a instância original ou para uma instância alternativa, com diferentes tipos de opções de recuperação e configurações disponíveis.

Antes de Iniciar

Certifique-se de que os requisitos a seguir sejam atendidos:

- Pelo menos uma tarefa de backup do Microsoft Exchange foi definida e executada com sucesso. Para obter instruções sobre como definir uma tarefa de backup, consulte [“Definindo uma tarefa de backup de Acordo de Nível de Serviço”](#) na página 165.
- As funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está definindo a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297.
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Importante: Para operações de restauração granular, deve-se efetuar logon no servidor de aplicativos Exchange e usar a GUI do Microsoft Management Console (MMC) para concluir tarefas do navegador de restauração em lote da caixa de correio e de restauração da caixa de correio.

Procedimento

Para restaurar dados em um banco de dados Microsoft Exchange, execute uma das seguintes ações:

- Restaurar um banco de dados para a instância e o local originais.
- Restaurar um banco de dados para a instância original com um local de arquivo diferente.
- Restaurar um banco de dados para uma instância alternativa.
- Restaurar dados da caixa de correio usando a função de restauração granular.
- Restaurar um banco de dados em um grupo de disponibilidade do banco de dados (DAG).

Restaurando um banco de dados Microsoft Exchange para a instância original

Restaure um banco de dados Microsoft Exchange para sua instância original usando o modo de produção ou o modo de teste. Escolha entre restaurar o backup mais recente ou uma versão anterior de backup de banco de dados do Exchange.

Antes de Iniciar

Certifique-se de que os requisitos a seguir sejam atendidos:

- Pelo menos uma tarefa de backup do Microsoft Exchange foi definida e executada com sucesso.
- As funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está definindo a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297.

Sobre Esta Tarefa

Ao restaurar um banco de dados para seu local original no modo de produção, não é possível renomeá-lo. Essa opção de restauração executa uma operação de restauração de produção completa e os dados existentes são sobrescritos no site de destino.

Procedimento

Para definir uma tarefa de restauração do Exchange, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Exchange > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Exchange**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados. Para remover um item da lista, clique no ícone de menos  próximo ao item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de Restauração	Selecione o tipo de tarefa de restauração: On-demand: Captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. On-demand: Momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.
Tipo de local da restauração	Selecione um tipo de local a partir do qual os dados serão restaurados: Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site . Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem . Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela

Opção	Descrição
	<p>Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.
Ponto de Restauração	Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
5. Na página **Método de restauração**, escolha a partir das opções a seguir:
 - **Teste** . No modo de teste, o agente cria um novo banco de dados usando os arquivos de dados diretamente do repositório do vSnap. Este tipo de restauração pode ser usado para propósitos de teste.
 - **Produção** . No modo de produção, primeiro o agente restaura os arquivos do volume vSnap de volta para o armazenamento primário e, em seguida, cria o novo banco de dados usando os arquivos restaurados.

Apenas para restauração de Teste, no campo **Novo nome do banco de dados**, insira o novo nome para o banco de dados restaurado. O campo **Novo nome do banco de dados** também é exibido quando

you choose restoration of Production, but this is for restoring to a new database location of data in the original instance. For detailed instructions on this task, consult [“Restaurando um banco de dados do Exchange para um novo local na instância original”](#) on page 172.

6. Optional: On the page **Opções da tarefa**, configure additional options for the restoration task and click on **Avançar** to continue.

Opções de Recuperação

Choose among the recovery options to follow:

Sem recuperação

This option ignores all Rollforward of recovery after the restoration operation. The database remains in a Rollforward pending state until you decide if you want to execute the Rollforward of recovery manually.

Recuperar até o término do backup

Restore the database selected for the state at the time of backup creation.

Recuperar até o término dos logs disponíveis

This option restores the database and applies all available logs (including more recent logs than the backup that may exist on the application server) to recover the database to the most recent possible moment. This option is available only if you have selected **Ativar backup do log** on the backup task.

Recuperar até um ponto específico no tempo

When log backups are enabled, this option restores the database and applies logs of the backup volume of log to recover the database to a specific intermediate moment, specified by the user. Choose the date and time by selecting from the options **Por Hora**.

Opções do Aplicativo

Configure the application options:

Máximo de Fluxos Paralelo por Banco de Dados

Configure the maximum number of parallel data flows of backup storage per database.

This configuration applies to each database in the task definition. Various databases can still be restored in parallel if the option value is configured as 1. The existence of multiple parallel flows can improve the restoration speed, but the high bandwidth consumption can affect the overall system performance.

This option is applicable only when restoring a database from Exchange to its original location using its original database name.

Opções Avançadas

Configure the advanced task definition options:

Executar limpeza imediatamente na falha da tarefa

Activate this option to automatically clean up resources allocated as part of a restoration, in case of a task failure.

7. Optional: On the page **Aplicar scripts**, select the **Pré-script** or the **Pós-Script** to be applied or choose **Continuar atividade/tarefa no erro de script**. For more information on how to work with scripts, consult [Configurando scripts](#). Click on **Avançar** to continue.
8. Execute one of the actions to follow on the page **Planejamento**:
 - If you are executing a task on demand, click on **Avançar**.
 - If you are configuring a recurring task, enter a name for the task scheduling and specify the frequency and when to start the restoration. Click on **Avançar**.
9. On the page **Revisar**, review your task configuration and click on **Enviar** to create the task.

The restoration task is created and it is possible to verify its status in **Tarefas e operações > Tarefas em execução**.

Restaurando um banco de dados do Exchange para um novo local na instância original

É possível restaurar um banco de dados Microsoft Exchange para sua instância original, mas para um novo local no servidor de aplicativos. Escolha entre restaurar o backup mais recente ou uma versão anterior de backup de banco de dados do Exchange.

Sobre Esta Tarefa

Ao restaurar um banco de dados para sua instância original usando uma operação de restauração de produção, é possível restaurar o banco de dados para um novo local de arquivo no servidor de aplicativos com um novo nome para o banco de dados restaurado. No modo de produção, o agente primeiro restaura os arquivos a partir do volume vSnap de volta para o armazenamento primário e, em seguida, cria um novo banco de dados usando os arquivos restaurados.

Procedimento

Para definir uma tarefa de restauração do Exchange, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Exchange > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Exchange**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados.

Para remover um item da lista, clique no ícone de menos  próximo ao item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de Restauração	Selecione o tipo de tarefa de restauração: On-demand: Captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. On-demand: Momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.

Opção	Descrição
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual os dados serão restaurados:</p> <p>Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.</p>
Ponto de Restauração	<p>Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
5. Na página **Método de restauração**, clique na opção de restauração **Produção**.

Dica: É obrigatório selecionar o modo de Produção para esta operação de restauração.

- a) No campo **Nome**, expanda o nome do banco de dados para ver as informações de caminho para o banco de dados existente no servidor de aplicativos.
 - b) No campo **Novo nome do banco de dados**, insira o novo nome para o banco de dados restaurado.
 - c) No campo **Caminho de destino**, inclua o novo local do arquivo de banco de dados do Exchange, incluindo o nome .edb e o local dos logs.
Por exemplo, para um banco de dados chamado Database_A.edb, insira C:\ExchangeDatabase\Database_A\Database_A.edb, e para o local dos logs (**Caminho de origem E01**), insira D:\ExchangeDatabase\Logs\Database_A\
6. Opcional: Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Opções de Recuperação

Escolha entre as opções de recuperação a seguir:

Sem recuperação

Esta opção ignora todo o Rollforward de recuperação após a operação de restauração. O banco de dados permanece em um estado Rollforward pending até que você decida se deseja executar o Rollforward de recuperação manualmente.

Recuperar até o término do backup

Restaure o banco de dados selecionado para o estado no momento da criação do backup.

Recuperar até o término dos logs disponíveis

Esta opção restaura o banco de dados e aplica todos os logs disponíveis (incluindo logs mais recentes do que o backup que pode existir no servidor de aplicativos) para recuperar o banco de dados até o momento mais recente possível. Esta opção estará disponível apenas se você tiver selecionado **Ativar backup do log** na tarefa de backup.

Recuperar até um ponto específico no tempo

Quando os backups de log estão ativados, esta opção restaura o banco de dados e aplica logs do volume de backup de log para recuperar o banco de dados até um momento intermediário, especificado pelo usuário. Escolha a data e hora selecionando a partir das opções **Por Hora**.

Opções do Aplicativo

Configure as opções do aplicativo:

Máximo de Fluxos Paralelo por Banco de Dados

Configure o máximo de fluxos de dados do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Vários bancos de dados ainda podem ser restaurados em paralelo se o valor da opção estiver configurado como 1. A existência de múltiplos fluxos paralelos pode melhorar a velocidade da restauração, mas o alto consumo de largura de banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas ao restaurar um banco de dados do Exchange para seu local original usando seu nome de banco de dados original.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Ative esta opção para limpar automaticamente os recursos alocados como parte de uma restauração, em caso de falha na recuperação.

7. Opcional: Na página **Aplicar scripts**, selecione o **Pré-script** ou o **Pós-Script** a ser aplicado ou escolha **Continuar atividade/tarefa no erro de script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#). Clique em **Avançar** para continuar.
8. Execute uma das ações a seguir na página **Planejamento**:
 - Se estiver executando uma tarefa on demand, clique em **Avançar**.

- Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.
- A tarefa de restauração é criada e é possível verificar seu status em **Tarefas e operações > Tarefas em execução**.

Restaurando um banco de dados Microsoft Exchange para uma instância alternativa

É possível selecionar um backup do banco de dados Microsoft Exchange e restaurá-lo para uma instância do Exchange Server em um host alternativo. É possível restaurar o banco de dados no modo de produção ou no modo de teste para a instância alternativa.

Antes de Iniciar

Certifique-se de que os seguintes requisitos sejam atendidos:

- O espaço em disco suficiente e os volumes dedicados alocados estão disponíveis para a cópia de arquivos.
- A estrutura do sistema de arquivos no servidor de origem é igual à estrutura do sistema de arquivos no servidor de destino. Esta estrutura de sistema de arquivos inclui espaços de tabela, logs on-line e o diretório de banco de dados local.

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Exchange > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Exchange**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.
As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados.
Para remover um item da lista, clique no ícone de menos  próximo ao item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de Restauração	<p>Selecione o tipo de tarefa de restauração:</p> <p>On-demand: Captura instantânea</p> <p>Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p>

Opção	Descrição
	<p>On-demand: Momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p> <p>Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.</p>
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual os dados serão restaurados:</p> <p>Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.</p>
Ponto de Restauração	<p>Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>

Opção	Descrição
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, escolha **Restaurar para uma instância alternativa**, selecione a instância de destino para a qual você deseja restaurar o banco de dados e, em seguida, clique em **Avançar**.
5. Na página **Método de restauração**, escolha a partir das opções a seguir:
 - **Teste** . No modo de teste, o agente cria um novo banco de dados usando os arquivos de dados diretamente do repositório do vSnap. Este tipo de restauração pode ser usado para propósitos de teste.
 - **Produção** . No modo de produção, primeiro o agente restaura os arquivos do volume vSnap de volta para o armazenamento primário e, em seguida, cria o novo banco de dados usando os arquivos restaurados.
 - a) No campo **Novo nome do banco de dados**, insira um novo nome do banco de dados.
 - b) (Apenas restauração de produção) Expanda o nome do banco de dados para ver as informações do caminho. No campo **Caminho de destino** , inclua o local do arquivo do banco de dados do Exchange no host alternativo, incluindo o nome .edb e o local dos logs.

Por exemplo, para um banco de dados chamado Database_A.edb, insira C:\ExchangeDatabase\Database_A\Database_A.edb para o local dos logs , enter c:\ExchangeDatabase\Logs\Database_A\
6. Opcional: Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Opções de Recuperação

Escolha entre as opções de recuperação a seguir:

Sem recuperação

Esta opção ignora todo o Rollforward de recuperação após a operação de restauração. O banco de dados permanece em um estado Rollforward pending até que você decida se deseja executar o Rollforward de recuperação manualmente.

Recuperar até o término do backup

Restaurar o banco de dados selecionado para o estado no momento da criação do backup.

Recuperar até o término dos logs disponíveis

Esta opção restaura o banco de dados e aplica todos os logs disponíveis (incluindo logs mais recentes do que o backup que pode existir no servidor de aplicativos) para recuperar o banco de dados até o momento mais recente possível. Esta opção estará disponível apenas se você tiver selecionado **Ativar backup do log** na tarefa de backup.

Recuperar até um ponto específico no tempo

Quando os backups de log estão ativados, esta opção restaura o banco de dados e aplica logs do volume de backup de log para recuperar o banco de dados até um momento intermediário, especificado pelo usuário. Escolha a data e hora selecionando a partir das opções **Por Hora** .

Opções do Aplicativo

Configure as opções do aplicativo:

Máximo de Fluxos Paralel por Banco de Dados

Configure o máximo de fluxos de dados do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Vários bancos de dados ainda podem ser restaurados em paralelo se o valor da opção estiver configurado como 1. A existência de múltiplos fluxos paralelos pode melhorar a velocidade da restauração, mas o alto consumo de largura de banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas ao restaurar um banco de dados do Exchange para seu local original usando seu nome de banco de dados original.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Ative esta opção para limpar automaticamente os recursos alocados como parte de uma restauração, em caso de falha na recuperação.

7. Opcional: Na página **Aplicar scripts**, selecione o **Pré-script** ou o **Pós-Script** a ser aplicado ou escolha **Continuar atividade/tarefa no erro de script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#). Clique em **Avançar** para continuar.
8. Execute uma das ações a seguir na página **Planejamento**:
 - Se estiver executando uma tarefa on demand, clique em **Avançar**.
 - Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

A tarefa de restauração é criada e é possível verificar seu status em **Tarefas e operações > Tarefas em execução**.

Restaurando itens individuais da caixa de correio usando uma operação de restauração granular

É possível restaurar itens individuais da caixa de correio do Microsoft Exchange usando uma operação de restauração granular e a GUI do Microsoft Management Console (MMC) do IBM Spectrum Protect Plus.

Antes de Iniciar

Deve-se ter permissões de controle de acesso baseado na função (RBAC) para concluir operações de restauração de caixa de correio individuais. Se as permissões de RBAC não foram designadas, é possível encontrar erros de configuração na GUI do MMC do IBM Spectrum Protect Plus para cada função ausente.

Dica:

Se você encontrar erros de configuração baseados na função na GUI do MMC do IBM Spectrum Protect Plus, será possível configurar as permissões necessárias manualmente para resolver os erros (consulte “Privilégios” na página 161), ou executar o assistente de configuração do IBM Spectrum Protect Plus para configurar permissões automaticamente (consulte a etapa “14” na página 181).

Sobre Esta Tarefa

Para iniciar uma operação de restauração granular, conclua as etapas preparatórias na GUI do IBM Spectrum Protect Plus e, em seguida, efetue login no servidor de aplicativos Exchange. Em seguida, use a GUI do MMC do IBM Spectrum Protect Plus para restaurar dados da caixa de correio do usuário do banco de dados de recuperação que é criado pela operação de restauração granular. Uma operação de restauração granular pode ser usada para concluir as seguintes tarefas:

- É possível restaurar itens da caixa de correio selecionada para a caixa de correio original, para outra caixa de correio on-line no mesmo servidor ou para um arquivo Unicode .pst.
- É possível restaurar um banco de dados da caixa de correio de pasta pública, uma caixa de correio de pasta pública ou apenas uma parte da caixa de correio, por exemplo, uma pasta pública específica.
- É possível restaurar uma caixa de correio de archive ou uma parte da caixa de correio, por exemplo, uma pasta específica.

- É possível restaurar mensagens da caixa de correio de archive para uma caixa de correio que está no Exchange Server , para uma caixa de correio de archive ou para um arquivo .pst do Exchange Server .

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Exchange > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Exchange**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar** .
 - b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração.

Dica: Apenas um banco de dados deve ser selecionado para uma operação de restauração granular. Caso vários bancos de dados sejam selecionados, a opção de restauração granular não estará disponível na página **Método de restauração**.

A origem selecionada é incluída na lista de restauração próxima à lista de bancos de dados. Para remover um item da lista, clique no ícone de menos  próximo ao item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de Restauração	<p>Selecione o tipo de tarefa de restauração:</p> <p>On-demand: Captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p> <p>On-demand: Momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p> <p>Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.</p>
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual os dados serão restaurados:</p> <p>Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p>

Opção	Descrição
	<p>Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.</p>
Ponto de Restauração	<p>Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
5. Na página **Método de restauração**, clique em **Restauração granular**.

O nome do banco de dados de recuperação é exibido no campo **Novo nome do banco de dados**. O nome consiste no nome do banco de dados existente com o sufixo **_RDB**.

6. Opcional: Na página **Opções da tarefa, Recuperar até o término do backup e Executar limpeza imediatamente na falha da tarefa** são selecionadas por padrão. Clique em **Avançar** para continuar.
7. Opcional: Na página **Aplicar scripts**, selecione o **Pré-script** ou o **Pós-Script** a ser aplicado ou escolha **Continuar atividade/tarefa no erro de script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#). Clique em **Avançar** para continuar.
8. Execute uma das ações a seguir na página **Planejamento**:
 - Se estiver executando uma tarefa on demand, clique em **Avançar**.
 - Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

A tarefa de restauração é criada e é possível verificar seu status em **Tarefas e operações > Tarefas em execução**.
10. Na área de janela de navegação, clique em **Tarefas e operações > Recursos ativos** para visualizar os detalhes do banco de dados de recuperação e do ponto de montagem.

Dica: Clique no ícone  para exibir uma mensagem de informação que descreve as próximas etapas para concluir a tarefa de restauração granular.
11. Conecte-se à instância do servidor de aplicativos Exchange usando a Conexão de Área de Trabalho Remota (RDC) ou a Virtual Network Computing (VNC) se estiver se conectando remotamente ou efetuando logon na máquina Exchange Server localmente.

A operação de restauração granular instala e inicia automaticamente a GUI de MMC do IBM Spectrum Protect Plus no servidor de aplicativos. Se a GUI do MMC falhar ao iniciar, inicie-a manualmente usando o caminho fornecido na mensagem de informação de **Recursos ativos**.
12. Na GUI do MMC do IBM Spectrum Protect Plus, clique no nó **Proteger e recuperar dados** e selecione **Exchange Server**.
13. Na guia **Recuperar** para a instância do Exchange Server, clique em **Visualizar > Mailbox Restore Browser** para visualizar a caixa de correio a partir do banco de dados de recuperação.
14. Opcional: Execute o assistente de configuração IBM Spectrum Protect Plus :
 - a) Na área de janela de navegação, clique em **Painel > Gerenciar > Configuração > Assistentes > IBM Spectrum Protect Plus Configuração**.
 - b) Na área de janela **Ações**, clique em **Iniciar**.

O assistente de configuração executa a verificação de requisitos.
 - c) Quando as verificações de requisitos foram executadas, clique no link **Avisos**, próximo a **Verificação de funções do usuário**.
 - d) Na caixa de diálogo de mensagem, para incluir quaisquer funções ausentes, clique em **Sim**.
 - e) No assistente de configuração, clique em **Avançar** e, em seguida, clique em **Concluir**.
15. Na árvore **Mailbox Restore Browser > Origem**, clique na caixa de correio que contém os itens que você deseja restaurar, o que permite procurar as pastas e mensagens individuais.

Escolha entre as seguintes ações para selecionar a pasta ou mensagem para restauração.

<i>Tabela 19. Visualizando e filtrando itens de caixa de correio</i>	
Tarefa	Ação
Visualizar itens da caixa de correio	<p>a. Selecione um item da caixa de correio, como Caixa de entrada, para exibir seus conteúdos na área de janela de visualização.</p> <p>b. Clique em um item individual na área de janela de visualização, como uma mensagem de e-mail, para visualizar o texto da mensagem e os detalhes.</p> <p>c. Se um item contiver um anexo, clique no ícone do anexo para visualizar seu conteúdo.</p>
Filtrar itens de caixa de correio	<p>Use as opções de filtro para limitar a lista de pastas e mensagens a serem restauradas:</p> <p>a. Clique em Mostrar Opções de Filtro e Incluir Linha.</p> <p>b. Clique na seta para baixo no campo Nome da Coluna e selecione um item a ser filtrado. É possível filtrar por nome de pasta, texto do assunto e outras opções.</p> <p>Restrição: É possível filtrar as pastas de caixa de correio públicas somente pela coluna Nome da Pasta.</p> <p>Ao selecionar Todo o Conteúdo, os itens da caixa de correio são filtrados pelo nome do anexo, o emissor, o assunto e o corpo da mensagem.</p> <p>c. No campo Operador, selecione um operador: Contém.</p> <p>d. No campo Valor, especifique um valor de filtro.</p> <p>e. Para especificar critérios de filtragem adicionais, clique em Incluir linha.</p> <p>f. Clique em Aplicar filtro para filtrar as mensagens e pastas.</p>

16. Quando tiver selecionado o item da caixa de correio para restauração, na área de janela **Ações**, clique na tarefa de restauração que deseja executar. Escolha entre as opções a seguir:

- **Restaurar Pasta para Caixa de Correio Original**
- **Restaurar Mensagens para Caixa de Correio Original**
- **Salvar Conteúdo da Mensagem de Correio**

Dica: Se você clicar em **Salvar conteúdo da mensagem de correio**, uma janela Salvar arquivo do Windows será exibida. Especifique o local e o nome da mensagem e clique em **Salvar**.

Ao escolher a opção de restauração, a janela **Progresso da restauração** é aberta e mostra o progresso da operação de restauração e o item da caixa de correio é restaurado.

17. Para restaurar um item de caixa de correio para outra caixa de correio ou arquivo .pst, conclua as seguintes etapas.

Nota: Também é possível restaurar uma caixa de correio completa para outra caixa de correio ou arquivo .pst.

Escolha entre as ações na tabela a seguir:

<i>Tabela 20. Restaurando um item de caixa de correio para outra caixa de correio ou arquivo .pst</i>	
Tarefa	Ação
Restaurar um item de caixa de correio (ou uma caixa de correio) para uma caixa de correio diferente	<p>a. Na área de janela Ações, clique em Abrir Caixa de Correio do Exchange.</p> <p>b. Insira o alias da caixa de correio para identificá-la como o destino da restauração.</p> <p>c. Arraste o item da caixa de correio de origem (ou caixa de correio) para a caixa de correio de destino na área de janela de resultados.</p> <p>Restrição: Não é possível arrastar itens de correio ou subpastas na pasta Itens Recuperáveis para uma caixa de correio de destino.</p>
Restaurar um item de caixa de correio (ou caixa de correio) para um arquivo de pastas pessoais do Outlook (.pst)	<p>a. Na área de janela Ações, clique em Abrir Arquivo PST não Unicode.</p> <p>b. Quando a janela Abrir arquivo for aberta, selecione um arquivo .pst existente ou crie um arquivo .pst.</p> <p>c. Arraste o item da caixa de correio de origem (ou caixa de correio) para o arquivo .pst de destino na área de janela de resultados.</p> <p>Restrição: É possível usar a visualização Navegador de restauração da caixa de correio apenas com arquivos .pst não Unicode.</p>

Tabela 20. Restaurando um item de caixa de correio para outra caixa de correio ou arquivo .pst (continuação)

Tarefa	Ação
Restaurar uma Pasta Pública	<p>Selecione esta ação para restaurar uma pasta pública para uma caixa de correio de pasta pública on-line existente.</p> <p>É possível filtrar a caixa de correio e restaurar uma pasta pública específica para uma pasta pública online existente. No campo Pasta a ser restaurada, insira o nome da pasta pública que você deseja restaurar.</p> <ul style="list-style-type: none"> • Para restaurar uma subpasta em uma pasta pai, especifique o caminho completo da pasta neste formato: <i>parent_folder_name/sub_folder_name</i>. • Para restaurar todas as subpastas em uma pasta pai, use <i>parent_folder_name/*</i>. • Se o caminho de pasta completo incluir espaços, coloque o caminho de pasta entre aspas duplas e não anexe um caractere de barra invertida (\). <p>Também é possível restaurar toda ou parte de uma pasta pública para uma caixa de correio de pasta pública diferente da caixa de correio original. No campo Caixa de correio de pasta pública de destino, especifique a caixa de correio de pasta pública de destino na qual deseja restaurar.</p>

18. Na área de janela **Ações**, clique em **Fechar caixa de correio do Exchange** ou **Fechar arquivo PST** para fechar a caixa de correio de destino ou o arquivo .pst.

Dica: É possível ativar o Microsoft Management Console para reunir informações de diagnóstico para ajudar na determinação de problema relacionados às operações de restauração. O processo reúne arquivos de configuração, arquivos de rastreamento e diagnósticos gerais da GUI do MMC. Para obter mais informações, consulte a nota técnica a seguir: [Ativando informações de diagnóstico na GUI MMC do IBM Spectrum Protect Plus](http://www.ibm.com/support/docview.wss?uid=ibm10882270)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>).

19. Quando a operação de restauração para os itens individuais for concluída, retorne para IBM Spectrum Protect Plus. Na área de janela **Tarefas e Operação > Recursos ativos**, clique em **Ações > Cancelar restauração granular** para terminar o processo de restauração granular.

Restaurando caixas de correio usando uma operação de restauração granular

É possível restaurar caixas de correio do Microsoft Exchange usando uma operação de restauração granular e a GUI do Microsoft Management Console (MMC) do IBM Spectrum Protect Plus.

Antes de Iniciar

Deve-se ter permissões de controle de acesso baseado na função (RBAC) para concluir operações de restauração de caixa de correio individuais. Se as permissões de RBAC não foram designadas, é possível encontrar erros de configuração na GUI do MMC do IBM Spectrum Protect Plus para cada função ausente.

Dica:

Se você encontrar erros de configuração baseados na função na GUI do MMC do IBM Spectrum Protect Plus, será possível configurar as permissões necessárias manualmente para resolver os erros (consulte

“Privilégios ” na página 161), ou executar o assistente de configuração do IBM Spectrum Protect Plus para configurar permissões automaticamente (consulte a etapa “14” na página 187).

Sobre Esta Tarefa

Para iniciar uma operação de restauração granular, conclua as etapas preparatórias na GUI do IBM Spectrum Protect Plus e, em seguida, efetue login no servidor de aplicativos Exchange. Em seguida, use a GUI do MMC do IBM Spectrum Protect Plus para restaurar dados da caixa de correio do usuário do banco de dados de recuperação criado pela operação de restauração granular. Uma operação de restauração granular pode ser usada para concluir as seguintes tarefas:

- É possível restaurar uma caixa de correio inteira ou itens da caixa de correio selecionada para a caixa de correio original, outra caixa de correio on-line no mesmo servidor ou para um arquivo Unicode .pst.
- É possível restaurar um banco de dados da caixa de correio de pasta pública, uma caixa de correio de pasta pública ou apenas uma parte da caixa de correio, por exemplo, uma pasta pública específica.
- É possível restaurar uma caixa de correio de archive ou uma parte da caixa de correio, por exemplo, uma pasta específica.
- É possível restaurar mensagens da caixa de correio de archive para uma caixa de correio que está no Exchange Server , para uma caixa de correio de archive ou para um arquivo .pst do Exchange Server .

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Exchange > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Exchange**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar** .

- b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração.

Dica: Apenas um banco de dados deve ser selecionado para uma operação de restauração granular. Caso vários bancos de dados sejam selecionados, a opção de restauração granular não estará disponível na página **Método de restauração**.

A origem selecionada é incluída na lista de restauração próxima à lista de bancos de dados. Para remover um item da lista, clique no ícone de menos  próximo ao item.

- c) Clique em **Avançar** para continuar.
3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de Restauração	Selecione o tipo de tarefa de restauração:

Opção	Descrição
	<p>On-demand: Captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p> <p>On-demand: Momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p> <p>Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.</p>
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual os dados serão restaurados:</p> <p>Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.</p>

Opção	Descrição
Ponto de Restauração	Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.
Usar servidor vSnap alternativo para a tarefa de restauração	Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo . Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

4. Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
5. Na página **Método de restauração**, clique em **Restauração granular**.
O nome do banco de dados de recuperação é exibido no campo **Novo nome do banco de dados**. O nome consiste no nome do banco de dados existente com o sufixo **_RDB**.
6. Opcional: Na página **Opções da tarefa**, **Recuperar até o término do backup** e **Executar limpeza imediatamente na falha da tarefa** são selecionadas por padrão. Clique em **Avançar** para continuar.
7. Opcional: Na página **Aplicar scripts**, selecione o **Pré-script** ou o **Pós-Script** a ser aplicado ou escolha **Continuar atividade/tarefa no erro de script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#). Clique em **Avançar** para continuar.
8. Execute uma das ações a seguir na página **Planejamento**:
 - Se estiver executando uma tarefa on demand, clique em **Avançar**.
 - Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.
A tarefa de restauração é criada e é possível verificar seu status em **Tarefas e operações > Tarefas em execução**.
10. Na área de janela de navegação, clique em **Tarefas e operações > Recursos ativos** para visualizar os detalhes do banco de dados de recuperação e do ponto de montagem.

Dica: Clique no ícone  para exibir uma mensagem de informação que descreve as próximas etapas para concluir a tarefa de restauração granular.
11. Conecte-se à instância do servidor de aplicativos Exchange usando a Conexão de Área de Trabalho Remota (RDC) ou a Virtual Network Computing (VNC) se estiver se conectando remotamente ou efetuando logon na máquina Exchange Server localmente.
A operação de restauração granular instala e inicia automaticamente a GUI de MMC do IBM Spectrum Protect Plus no servidor de aplicativos. Se a GUI do MMC falhar ao iniciar, inicie-a manualmente usando o caminho fornecido na mensagem de informação de **Recursos ativos**.
12. Na GUI do MMC do IBM Spectrum Protect Plus, clique no nó **Proteger e recuperar dados** e selecione **Exchange Server**.
13. Na guia **Recuperação** para a instância do Exchange Server, selecione **Visualizar > Restauração da caixa de correio**.
É exibida uma lista de caixas de correio do usuário de todos os bancos de dados que estão incluídos no backup.
14. Opcional: Execute o assistente de configuração IBM Spectrum Protect Plus :

- a) Na área de janela de navegação, clique em **Painel > Gerenciar > Configuração > Assistentes > IBM Spectrum Protect Plus Configuração**.
- b) Na área de janela **Ações**, clique em **Iniciar**.
O assistente de configuração executa a verificação de requisitos.
- c) Quando as verificações de requisitos foram executadas, clique no link **Avisos**, próximo a **Verificação de funções do usuário**.
- d) Na caixa de diálogo de mensagem, para incluir quaisquer funções ausentes, clique em **Sim**.
- e) No assistente de configuração, clique em **Avançar** e, em seguida, clique em **Concluir**.
15. Selecione uma ou mais caixas de correio a partir do banco de dados de recuperação para restaurar. As caixas de correio são listadas por Nome da caixa de correio, Alias, Servidor, Banco de dados e Tipo de caixa de correio.
É possível restaurar apenas as caixas de correio do usuário que estão localizadas no banco de dados de recuperação.
- Dica:** As caixas de correio de outros bancos de dados são mostradas nesta visualização apenas para propósitos informativos. Se a caixa de correio que você deseja restaurar não estiver no banco de dados de recuperação, use esta visualização para determinar a qual banco de dados Exchange a caixa de correio do usuário foi designada. É possível, então, executar a tarefa de restauração granular novamente para esse banco de dados.
16. Para concluir a operação de restauração, na área de janela **Ações**, clique em uma das seguintes opções de restauração.

<i>Tabela 21. Opções de Restauração</i>	
Opção	Ação
Restaurar Correio para Local Original	Restaurar os itens de correio para seu local no momento da operação de backup.
Restaurar Correio para Local Alternativo	Restaurar os itens de correio para uma caixa de correio diferente. <ul style="list-style-type: none"> Na janela Opções de caixa de correio alternativa, insira o nome do Alias da caixa de correio. <p>Dica: Se itens de correio ou tarefas excluídos são sinalizados na pasta Itens recuperáveis de uma caixa de correio, os itens são restaurados com o atributo de sinalização para a visualização Itens e tarefas sinalizados na caixa de correio de destino.</p>
Restaurar Correio para o Arquivo PST Não Unicode Restrição: <ul style="list-style-type: none"> Esta opção está disponível apenas para o Exchange Server 2013. Cada pasta pode conter um máximo de 16.383 itens de correio. 	Restaurar itens de correio para um arquivo de pastas pessoais não Unicode (.pst). Ao restaurar itens de correio para um arquivo .pst com uma caixa de correio selecionada, é solicitado um nome de arquivo. Ao restaurar itens de correio para um arquivo .pst com mais de uma caixa de correio selecionada, é solicitado um local de diretório. Cada caixa de correio é restaurada para um arquivo .pst separado que reflete o nome da caixa de correio no diretório especificado. Se o arquivo .pst já existir, o arquivo será usado. Caso contrário, o arquivo será criado.

Tabela 21. Opções de Restauração (continuação)

Opção	Ação
<p>Restaurar Correio para o Arquivo PST Unicode</p>	<p>Restaure itens de correio para um arquivo .pst Unicode.</p> <p>Ao restaurar itens de correio para um arquivo .pst com uma caixa de correio selecionada, é solicitado um nome de arquivo. Ao restaurar itens de correio para um arquivo .pst com mais de uma caixa de correio selecionada, é solicitado um local de diretório.</p> <p>Dica:</p> <p>Você pode digitar um nome de caminho padrão (por exemplo, c:\PST\mailbox.pst) ou um caminho de UNC (por exemplo, \\server\c\$\PST\mailbox.pst). Quando você digita um caminho padrão, o caminho é convertido em um caminho UNC. Se o UNC é um caminho UNC padrão, digite o caminho UNC diretamente.</p> <p>Cada caixa de correio é restaurada para um arquivo .pst separado que reflete o nome da caixa de correio no diretório especificado. Se o arquivo .pst já existir, o arquivo será usado. Caso contrário, o arquivo será criado.</p>
<p>Restaurar Caixa de Correio de Pasta Pública</p>	<p>Restaure uma caixa de correio de pasta pública para uma caixa de correio de pasta pública on-line.</p> <p>No campo Pasta a ser restaurada, insira o nome da pasta pública que você deseja restaurar:</p> <ul style="list-style-type: none"> • Para restaurar uma subpasta em uma pasta pai, especifique o caminho completo da pasta neste formato: <i>parent_folder_name/sub_folder_name</i>. • Para restaurar todas as subpastas em uma pasta pai, use <i>parent_folder_name/*</i>. • Se o caminho de pasta completo incluir espaços, coloque o caminho de pasta entre aspas duplas e não anexe um caractere de barra invertida (\). <p>Também é possível restaurar toda ou parte de uma caixa de correio de pasta pública para uma caixa de correio de pasta pública diferente da caixa de correio original. No campo Caixa de correio de pasta pública de destino, especifique a caixa de correio de pasta pública de destino.</p>

Tabela 21. Opções de Restauração (continuação)	
Opção	Ação
Restaurar Correio para Caixa de Correio de Archive	<p>Essa ação se aplica a uma caixa de correio primária ou uma caixa de correio de archive. Selecione esta ação para restaurar todo ou parte de qualquer tipo de caixa de correio para a caixa de correio de archive original ou para uma caixa de correio de archive alternativa.</p> <p>É possível filtrar a caixa de correio de archive e restaurar uma pasta de caixa de correio específica. No campo Pasta a ser restaurada, insira o nome da pasta na caixa de correio de archive que você deseja restaurar.</p> <ul style="list-style-type: none"> • Para restaurar uma subpasta em uma pasta pai, especifique o caminho completo da pasta neste formato: <i>parent_folder_name/sub_folder_name</i>. • Para restaurar todas as subpastas em uma pasta pai, use <i>parent_folder_name/*</i>. • Se o caminho de pasta completo incluir espaços, coloque o caminho de pasta entre aspas duplas e não anexe um caractere de barra invertida (\). <p>No campo Caixa de correio de archive de destino, especifique o destino da caixa de correio de archive.</p>
Excluir itens de correio recuperáveis durante restauração da caixa de correio	<p>Aplique esta ação se estiver restaurando uma caixa de correio on-line, de pública ou de archive para uma caixa de correio original, uma caixa de correio alternativa ou para um arquivo .pst Unicode.</p> <p>Especifique um valor de Yes para excluir os itens de correio na pasta Itens Recuperáveis em operações de restauração de caixa de correio. No é o valor padrão.</p>

Dica: É possível ativar o Microsoft Management Console para reunir informações de diagnóstico para ajudar na determinação de problema relacionados às operações de restauração. O processo reúne arquivos de configuração, arquivos de rastreamento e diagnósticos gerais da GUI do MMC. Para obter mais informações, consulte a nota técnica a seguir: [Ativando informações de diagnóstico na GUI MMC do IBM Spectrum Protect Plus](http://www.ibm.com/support/docview.wss?uid=ibm10882270)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>).

17. Quando a operação de restauração da caixa de correio estiver concluída, retorne para o IBM Spectrum Protect Plus. Na área de janela **Tarefas e Operação > Recursos ativos**, clique em **Ações > Cancelar restauração granular** para terminar o processo de restauração granular.

Restaurando Backups do Database Availability Group

Com o IBM Spectrum Protect Plus, é possível restaurar um backup do Grupo de Disponibilidade do Banco de Dados (DAG) do Exchange Server para a instância original ou para uma instância alternativa.

Sobre Esta Tarefa

Em um ambiente DAG, deve-se restaurar um banco de dados para uma cópia do banco de dados ativo. Se você selecionou uma cópia do banco de dados passivo como o destino preferencial de operações de backup, o IBM Spectrum Protect Plus tentará restaurar o banco de dados para essa cópia passiva por padrão. Falha na operação de restauração. Nessa situação, é possível optar por restaurar o banco de dados para uma instância alternativa e, em seguida, selecionar a cópia do banco de dados ativo.

Procedimento

Para definir uma tarefa de restauração do Exchange, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Exchange > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Exchange**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Selecionar origem**, conclua as etapas a seguir:
 - a) Clique no menu **Visualizar** e selecione **Grupos de disponibilidade do banco de dados**.
 - b) Na lista **Grupos de disponibilidade**, clique em uma instância do Exchange para ver a lista de pontos de restauração para essa instância e selecione as versões de backup que você deseja restaurar. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - c) Clique no ícone Incluir na lista de restauração  ao lado do banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados. Para remover um item da origem da lista, clique no ícone  ao lado do item.
 - d) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de Restauração	Selecione o tipo de tarefa de restauração: On-demand: Captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. On-demand: Momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.
Tipo de local da restauração	Selecione um tipo de local a partir do qual os dados serão restaurados: Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site . Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem .

Opção	Descrição
	<p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.</p>
Ponto de Restauração	<p>Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, especifique onde deseja restaurar o banco de dados e clique em **Avançar.**

Restaurar para a instância original

Selecione essa opção para restaurar o banco de dados para o servidor original.

Restaurar para instância alternativa

Selecione essa opção para restaurar o banco de dados para um destino local que seja diferente da instância original e, em seguida, selecione o local alternativo a partir da lista de servidores disponíveis.



Atenção: Ao escolher o destino, deve-se selecionar um nó ativo como o destino; caso contrário, a operação de restauração falhará.

5. Na página **Método de restauração**, escolha a partir das opções a seguir:

- **Teste** . Escolha esta opção para restaurar os dados diretamente do repositório do vSnap. Este tipo de restauração pode ser usado para propósitos de teste.
- **Produção** . Escolha esta opção para restaurar o banco de dados completo com uma operação de restauração completa de dados de cópia. Essa operação de restauração é para uso permanente do banco de dados restaurado.

Clique em **Avançar** para continuar.

6. Opcional: Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Opções de Recuperação

Escolha entre as opções de recuperação a seguir:

Sem recuperação

Esta opção ignora todo o Rollforward de recuperação após a operação de restauração. O banco de dados permanece em um estado Rollforward pending até que você decida se deseja executar o Rollforward de recuperação manualmente.

Recuperar até o término do backup

Restaure o banco de dados selecionado para o estado no momento da criação do backup.

Recuperar até o término dos logs disponíveis

Esta opção restaura o banco de dados e aplica todos os logs disponíveis (incluindo logs mais recentes do que o backup que pode existir no servidor de aplicativos) para recuperar o banco de dados até o momento mais recente possível. Esta opção estará disponível apenas se você tiver selecionado **Ativar backup do log** na tarefa de backup.

Recuperar até um ponto específico no tempo

Quando os backups de log estão ativados, esta opção restaura o banco de dados e aplica logs do volume de backup de log para recuperar o banco de dados até um momento intermediário, especificado pelo usuário. Escolha a data e hora selecionando a partir das opções **Por Hora** .

Opções do Aplicativo

Configure as opções do aplicativo:

Máximo de Fluxos Paralelo por Banco de Dados

Configure o máximo de fluxos de dados do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Vários bancos de dados ainda podem ser restaurados em paralelo se o valor da opção estiver configurado como 1. A existência de múltiplos fluxos paralelos pode melhorar a velocidade da restauração, mas o alto consumo de largura de banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas ao restaurar um banco de dados do Exchange para seu local original usando seu nome de banco de dados original.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Ative esta opção para limpar automaticamente os recursos alocados como parte de uma restauração, em caso de falha na recuperação.

7. Opcional: Na página **Aplicar scripts**, selecione o **Pré-script** ou o **Pós-Script** a ser aplicado ou escolha **Continuar atividade/tarefa no erro de script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#). Clique em **Avançar** para continuar.

8. Execute uma das ações a seguir na página **Planejamento**:
 - Se estiver executando uma tarefa on demand, clique em **Avançar**.
 - Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.
A tarefa de restauração é criada e é possível verificar seu status em **Tarefas e operações > Tarefas em execução**.

Acessando arquivos de banco de dados do Exchange com o modo de acesso instantâneo

É possível acessar os arquivos de banco de dados do Microsoft Exchange usando o tipo de restauração de acesso instantâneo e montar os arquivos do banco de dados a partir do volume vSnap para um servidor de aplicativos.

Sobre Esta Tarefa

No modo de acesso instantâneo, nenhuma ação adicional será executada após o IBM Spectrum Protect Plus montar o compartilhamento. Use os dados para recuperação customizada de dados dos arquivos no volume vSnap.

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Exchange > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Exchange**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.
As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados.
Para remover um item da lista, clique no ícone de menos  próximo ao item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de Restauração	<p>Selecione o tipo de tarefa de restauração:</p> <p>On-demand: Captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p>

Opção	Descrição
	<p>On-demand: Momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente.</p> <p>Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.</p>
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual os dados serão restaurados:</p> <p>Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.</p>
Ponto de Restauração	<p>Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>

Opção	Descrição
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, especifique onde você deseja montar os arquivos de banco de dados e clique em **Avançar**.

Opção	Descrição
Restaurar para o local original	Selecione esta opção para montar os arquivos de banco de dados no servidor original.
Restaurar o local alternativo	Selecione essa opção para montar os arquivos do banco de dados em um destino local que seja diferente do servidor original e, em seguida, selecione o local alternativo na lista de servidores disponíveis.

5. Na página **Método de restauração**, escolha **Acesso instantâneo** e, em seguida, clique em **Avançar**.
6. Opcional: Na página **Opções da tarefa**, configure as opções adicionais, se necessário e clique em **Avançar** para continuar.
7. Opcional: Na página **Aplicar scripts**, selecione o **Pré-script** ou o **Pós-Script** a ser aplicado ou escolha **Continuar atividade/tarefa no erro de script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte [Configurando scripts](#). Clique em **Avançar** para continuar.
8. Execute uma das ações a seguir na página **Planejamento**:
- Se estiver executando uma tarefa on demand, clique em **Avançar**.
 - Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.
- A tarefa de restauração é criada e é possível verificar seu status em **Tarefas e operações > Tarefas em execução**.
10. Agora é possível acessar os arquivos do banco de dados do Exchange no ponto de montagem do servidor de aplicativos e executar quaisquer ações relacionadas ou customizadas do Exchange que você desejar.
- Nota:** Os arquivos de banco de dados do Exchange no ponto de montagem são leitura/gravação. No entanto, atualizá-los não modifica o backup original.
11. Quando tiver concluído a operação de restauração de acesso instantâneo, acesse a área de janela **Recursos ativos** e clique em **Ações > Cancelar restauração** para remover o banco de dados montado e terminar o processo de restauração.

MongoDB

Depois de incluir com sucesso instâncias do MongoDB no IBM Spectrum Protect Plus, é possível começar a proteger os dados em bancos de dados MongoDB. Crie políticas de acordo de nível de serviço (ANS) para fazer backup e manter dados do MongoDB.

Certifique-se de que o ambiente MongoDB atenda aos requisitos do sistema. Para obter mais informações, consulte [“Requisitos do MongoDB” na página 34](#).

Pré-requisitos para o MongoDB

Todos os requisitos e pré-requisitos do sistema para o IBM Spectrum Protect Plus Servidor de aplicativos MongoDB devem ser atendidos antes de começar a proteção dos dados do MongoDB com o IBM Spectrum Protect Plus.

Para requisitos do sistema MongoDB, consulte [Requisitos do sistema MongoDB](#).

Para atender aos pré-requisitos para o MongoDB, conclua as seguintes verificações e ações.

1. Certifique-se de que tenha atendido aos requisitos de espaço, conforme descrito em [Requisitos de espaço para proteção do MongoDB](#).
2. Configure o limite de tamanho do arquivo para o usuário da instância do MongoDB com o comando **ulimit -f** para ilimitado. Como alternativa, configure o valor como suficientemente alto para permitir a cópia dos maiores arquivos de banco de dados nas tarefas de backup e restauração. Se você mudar a configuração **ulimit**, reinicie a instância do MongoDB para finalizar a configuração.
3. Se estiver executando o MongoDB em um ambiente AIX ou Linux, certifique-se de que a versão do sudo instalada esteja em um nível suportado.

Para obter informações adicionais sobre o nível de versão, consulte [“Requisitos do MongoDB” na página 34](#). Para obter informações sobre como configurar privilégios sudo, consulte [“Configurando Privilégios Sudo” na página 199](#).

4. Se seus bancos de dados MongoDB estiverem protegidos por autenticação, deve-se configurar o controle de acesso baseado na função. Para obter mais informações, consulte [“Roles para MongoDB” na página 197](#).
5. Cada instância do MongoDB a ser protegida deve ser registrada no IBM Spectrum Protect Plus. Depois que as instâncias forem registradas, o IBM Spectrum Protect Plus executará um inventário para detectar recursos do MongoDB. Certifique-se de que todas as instâncias que você deseja proteger sejam detectadas e listadas corretamente.
6. Certifique-se de que o serviço SSH esteja em execução na porta 22 no servidor e que os firewalls estejam configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor com SSH. O subsistema SFTP para SSH deve ser ativado.
7. Certifique-se de não configurar pontos de montagem aninhados.

Restrições

As restrições a seguir se aplicam ao servidor de aplicativos MongoDB:

- As configurações de cluster fragmentadas do MongoDB são detectadas durante a execução de um inventário, mas esses recursos não são elegíveis para operações de backup ou restauração.
- Os caracteres Unicode em nomes de caminhos de arquivo do MongoDB não podem ser manipulados pelo IBM Spectrum Protect Plus. Todos os nomes devem estar em ASCII.

Virtualização

Proteja seu ambiente MongoDB com o IBM Spectrum Protect Plus quando ele estiver em execução em um dos seguintes sistemas operacionais guest:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server Kernel-based Virtual Machine (KVM)

Roles para MongoDB

Deve-se definir funções de controle de acesso baseado na função (RBAC) para os usuários do agente do MongoDB se a autenticação estiver ativada no banco de dados MongoDB. Quando as funções estiverem configuradas, os usuários poderão proteger e monitorar recursos do MongoDB com o IBM Spectrum Protect Plus, de acordo com as funções definidas dos usuários.

Controle de acesso baseado em função para MongoDB

Para cada usuário do MongoDB, especifique funções de acesso usando um comando semelhante ao seguinte exemplo:

```
use admin
db.grantRolesToUser ("< username>",
[ { role: "hostManager", db: "admin" },
{ role: "clusterManager", db: "admin" } ] )
```

As funções a seguir estão disponíveis:

hostManager

Essa função fornece acesso ao comando **fsyncLock**. Este acesso é necessário para backups consistentes do aplicativo de bancos de dados MongoDB, nos quais o registro no diário não está ativado. Essa função também fornece acesso ao comando de encerramento, que é usado durante uma operação de restauração para encerrar a instância do servidor MongoDB para a qual a restauração é direcionada.

clusterMonitor

Essa função fornece acesso a comandos para monitorar e ler o estado do banco de dados MongoDB. Os seguintes comandos estão disponíveis para usuários com esta função:

- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

clusterManager

Esta função é necessária somente para executar operações de restauração de teste de conjuntos de réplicas. Os usuários que executam o comando **replSetReconfig** podem criar a instância restaurada de um conjunto de réplicas de nó único. Essa função permite acesso de leitura e gravação durante as operações de restauração de teste de conjuntos de réplicas. Sem esse acesso, o nó no conjunto de réplicas permaneceria no estado REMOVED sem acesso de leitura e gravação. Além disso, essa função fornece acesso a comandos para a leitura do estado do banco de dados MongoDB. Os seguintes comandos estão disponíveis para esta função:

- **replSetReconfig**
- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

Pré-requisitos de espaço para a proteção de MongoDB

Antes de iniciar o backup de dados do MongoDB, certifique-se de que tenha espaço livre suficiente nos hosts de destino e de origem e no repositório do vSnap. É necessário espaço extra para armazenar backups temporários do Gerenciador de Volume Lógico (LVM) de volumes lógicos nos quais os dados do MongoDB estão localizados. Esses backups temporários, que são conhecidos como capturas instantâneas do LVM, são criados automaticamente pelo agente do MongoDB.

Capturas instantâneas do LVM

Capturas instantâneas do LVM são cópias point-in-time de volumes lógicos do LVM. Após a conclusão da operação de cópia de arquivo, as capturas instantâneas do LVM anteriores são removidas pelo agente do IBM Spectrum Protect Plus MongoDB em uma operação de limpeza.

Para cada volume lógico de captura instantânea do LVM, você deve alocar pelo menos 10 por cento de espaço livre no grupo de volumes. Se houver espaço livre suficiente no grupo de volumes, o agente do IBM Spectrum Protect Plus MongoDB reservará até 25 por cento do tamanho do volume lógico de origem para o volume lógico de captura instantânea.

Linux LVM2

Quando uma operação de backup do MongoDB é executada, o MongoDB solicita uma captura instantânea. Essa captura instantânea é criada em um sistema Logical Volume Management (LVM) para cada volume lógico com dados ou logs para o banco de dados selecionado. Em sistemas Linux, os volumes lógicos são gerenciados pelo LVM2.

Uma captura instantânea LVM2 baseada em software é obtida como um novo volume lógico no mesmo grupo de volumes. Os volumes de captura instantânea são montados temporariamente na mesma máquina que executa a instância do MongoDB para que eles possam ser transferidos para o repositório do vSnap.

No Linux, o gerenciador de volume LVM2 armazena a captura instantânea de um volume lógico no mesmo grupo de volumes. Deve haver espaço suficiente disponível para armazenar o volume lógico. O volume lógico cresce em tamanho conforme os dados mudam no volume de origem durante o tempo de vida da captura instantânea.

Configurando Privilégios Sudo

Para usar o IBM Spectrum Protect Plus para proteger seus dados, você deve instalar a versão necessária do programa sudo.

Sobre Esta Tarefa

Configure um usuário do agente dedicado do IBM Spectrum Protect Plus com os privilégios de superusuário necessários para sudo. Essa configuração permite que os usuários do agente executem comandos sem uma senha.

Procedimento

1. Crie um usuário do agente emitindo o seguinte comando:

```
useradd -m agent
```

em que *agent* especifica o nome do usuário do agente do IBM Spectrum Protect Plus.

2. Configure uma senha para o novo usuário emitindo o seguinte comando:

```
passwd mongodb_agent
```

3. Para ativar privilégios de superusuário para o usuário do agente, defina a configuração `!requiretty`. No final do arquivo de configuração sudo, inclua as seguintes linhas:

```
Padrões: agent ! requiretty
agent ALL=(ALL) NOPASSWD:ALL
```

Como alternativa, se seu arquivo sudoers estiver configurado para importar configurações de outro diretório, por exemplo, `/etc/sudoers.d`, é possível incluir as linhas no arquivo apropriado nesse diretório.

Incluindo um servidor de aplicativos MongoDB

Para começar a proteger recursos do MongoDB, deve-se incluir o servidor que hospeda as instâncias do MongoDB e configurar credenciais para as instâncias. Repita o procedimento para incluir todos os servidores que hospedam recursos do MongoDB.

Sobre Esta Tarefa

Para incluir um servidor de aplicativos MongoDB no IBM Spectrum Protect Plus, deve-se ter o endereço do host da máquina.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > MongoDB**.
2. Na janela **MongoDB**, clique em **Gerenciar servidores de aplicativos** e clique em **Incluir servidor de aplicativos** para incluir a máquina host.



3. No formulário **Propriedades do aplicativo**, insira o endereço do host.
4. Escolha registrar o host com um usuário ou uma chave SSH.

Se você selecionar **Usuário**, será possível optar por inserir um novo usuário e senha, ou um usuário existente. Se você selecionar **Chave SSH**, selecione a chave SSH no menu.

Restrição: Qualquer usuário que estiver especificado deve ter privilégios sudo configurados.

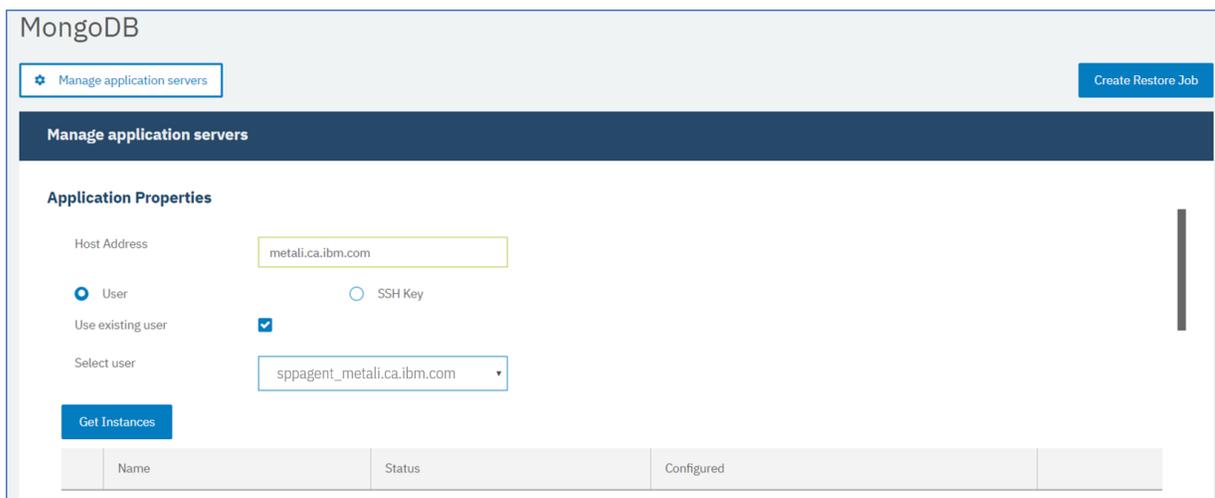


Figura 25. Incluindo um agente MongoDB

5. Clique em **Obter instâncias** para detectar e listar as instâncias do MongoDB que estão disponíveis no servidor host que está sendo incluído.

Cada instância do MongoDB é listada com seu endereço do host de conexão, status e uma indicação se ela está configurada.



Atenção: Se você registrar mais de um servidor de aplicativos para um conjunto de réplicas, o nome da instância que será exibido poderá ser mudado após cada operação de inventário, backup ou restauração. O nome do host do servidor de aplicativos incluído mais recentemente que pertence ao conjunto de réplicas é usado como parte do nome da instância. Uma operação de inventário é executada como parte das operações de backup e restauração.

6. Se estiver usando o controle de acesso, configure uma instância configurando credenciais. Clique em **Configurar credencial** e configure o ID do usuário e a senha. Como alternativa, é possível selecionar para usar um perfil do usuário existente.

Para obter informações adicionais sobre controle de acesso, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297.

Ao configurar credenciais, você designa funções de usuário do MongoDB para operações de backup e restauração com acesso a servidores MongoDB protegidos por função usando Salted Challenge Response Authentication Mechanism (SCRAM) ou Autenticação de desafio e resposta. O usuário do MongoDB designado para o servidor MongoDB protegido por função requer um dos seguintes níveis de acesso para proteger recursos:

- *Gerenciador de host:* Gerencia o banco de dados como o administrador. Esta função é necessária para obter e gerenciar capturas instantâneas.

- *Administrador de cluster*: Recupera informações de configuração e executa operações de restauração de modo de teste de conjuntos de réplicas do MongoDB. Esta função é necessária para reconfigurar operações de restauração de modo de teste de conjuntos de réplicas do MongoDB para consultas de dados.
 - *Monitor do cluster*: Monitora a proteção de recursos do MongoDB e recupera informações de configuração.
7. Opcional: Configure a opção **Máximo de bancos de dados simultâneos** inserindo um número no campo.
 8. Salve o formulário e repita as etapas para incluir outros servidores de aplicativos MongoDB no IBM Spectrum Protect Plus.

O que Fazer Depois

Depois de incluir servidores de aplicativos MongoDB no IBM Spectrum Protect Plus, um inventário é executado automaticamente em cada servidor de aplicativos para detectar os bancos de dados relevantes nessas instâncias.

Para verificar se os bancos de dados foram incluídos, revise o log da tarefa. Acesse **Tarefas e operações**. Clique na guia **Tarefas em execução** e procure a entrada de log Inventário do servidor de aplicativos mais recente.

As tarefas concluídas são mostradas na guia **Histórico da tarefa**. É possível usar a lista **Classificar por** para classificar tarefas com base no horário de início, no tipo, no status, no nome ou na duração da tarefa. Use o campo **Procurar por nome** para procurar tarefas por nome. É possível usar asteriscos como um curinga no nome.

Os bancos de dados devem ser detectados para assegurar que possam estar protegidos. Para obter instruções sobre como executar um inventário manual, consulte [Detectando recursos do MongoDB](#).

Detectando recursos do MongoDB

Depois de incluir servidores de aplicativos MongoDB no IBM Spectrum Protect Plus, um inventário é executado automaticamente para detectar todas as instâncias e bancos de dados MongoDB. É possível executar um inventário manual em qualquer servidor de aplicativos para detectar, listar e armazenar todos os bancos de dados MongoDB para o host selecionado.

Antes de Iniciar

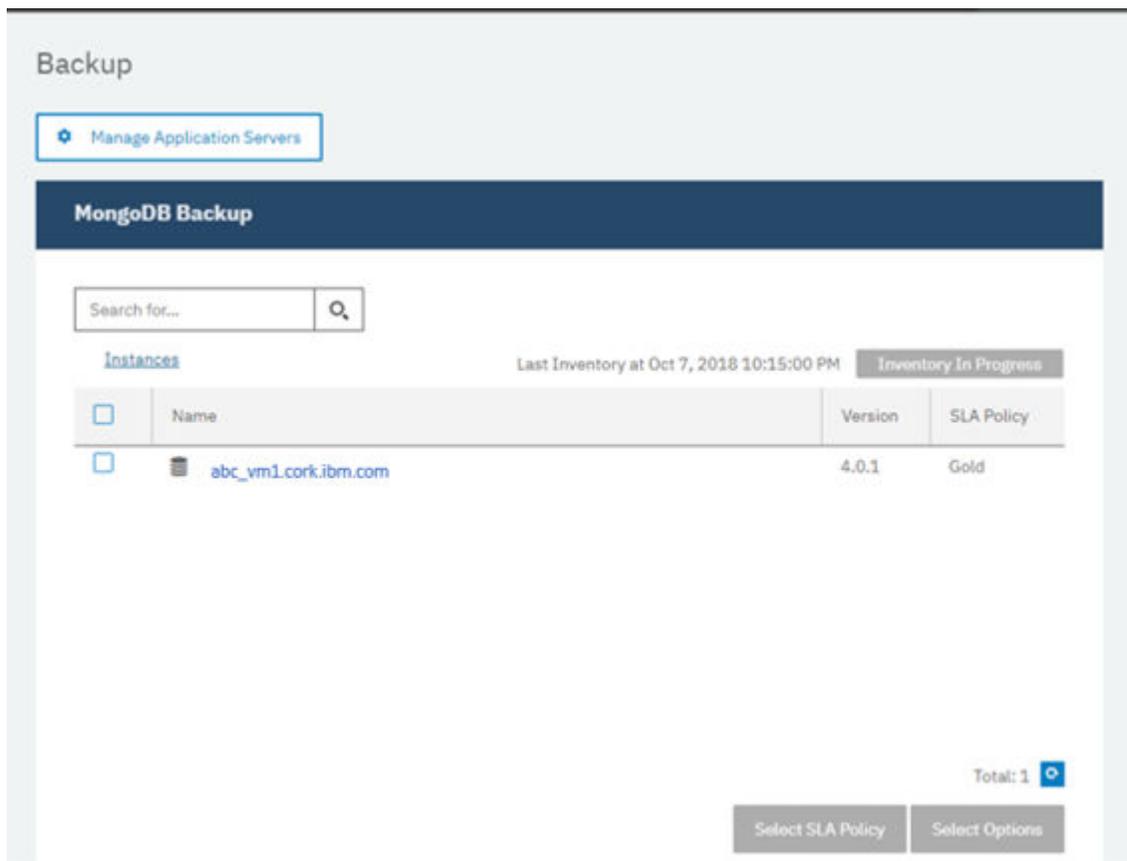
Certifique-se de que tenha incluído servidores de aplicativos MongoDB no IBM Spectrum Protect Plus. Para obter instruções, consulte [Incluindo um servidor de aplicativos MongoDB](#).

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > MongoDB**.

Dica: Para incluir mais instâncias do MongoDB na área de janela **Instâncias**, siga as instruções em [Incluindo um servidor de aplicativos MongoDB](#).

2. Clique em **Executar inventário**.



Quando o inventário estiver em execução, o botão muda para **Inventário em andamento**. É possível executar um inventário em quaisquer servidores de aplicativos disponíveis, mas é possível executar somente um processo de inventário por vez.

Para monitorar a tarefa de inventário, acesse **Tarefas e operações**. Clique na guia **Tarefas em execução** e procure a entrada do log Inventário do servidor de aplicativos mais recente.

As tarefas concluídas são mostradas na guia **Histórico da tarefa**. É possível usar a lista **Classificar por** para classificar tarefas com base no horário de início, no tipo, no status, no nome ou na duração da tarefa. Use o campo **Procurar por nome** para procurar tarefas por nome. É possível utilizar asteriscos como caracteres curinga no nome.

3. Clique em uma instância para abrir uma visualização que mostra os bancos de dados que são detectados para essa instância. Se algum banco de dados estiver ausente na lista **Instâncias**, verifique seu servidor de aplicativos MongoDB e execute o inventário novamente. Em alguns casos, alguns bancos de dados são marcados como inelegíveis para backup; passe o mouse sobre o banco de dados para revelar a razão disso.

Dica: Para retornar à lista de instâncias, clique no link **Instâncias** na área de janela **Fazer backup do MongoDB**.



Atenção: Se você registrar mais de um servidor de aplicativos para um conjunto de réplicas, o nome da instância que será exibido poderá ser mudado após cada operação de inventário, backup ou restauração. O nome do host do servidor de aplicativos com inventário mais recente que pertence ao conjunto de réplicas é usado como parte do nome da instância. Uma operação de inventário é executada como parte das operações de backup e restauração.

O que Fazer Depois

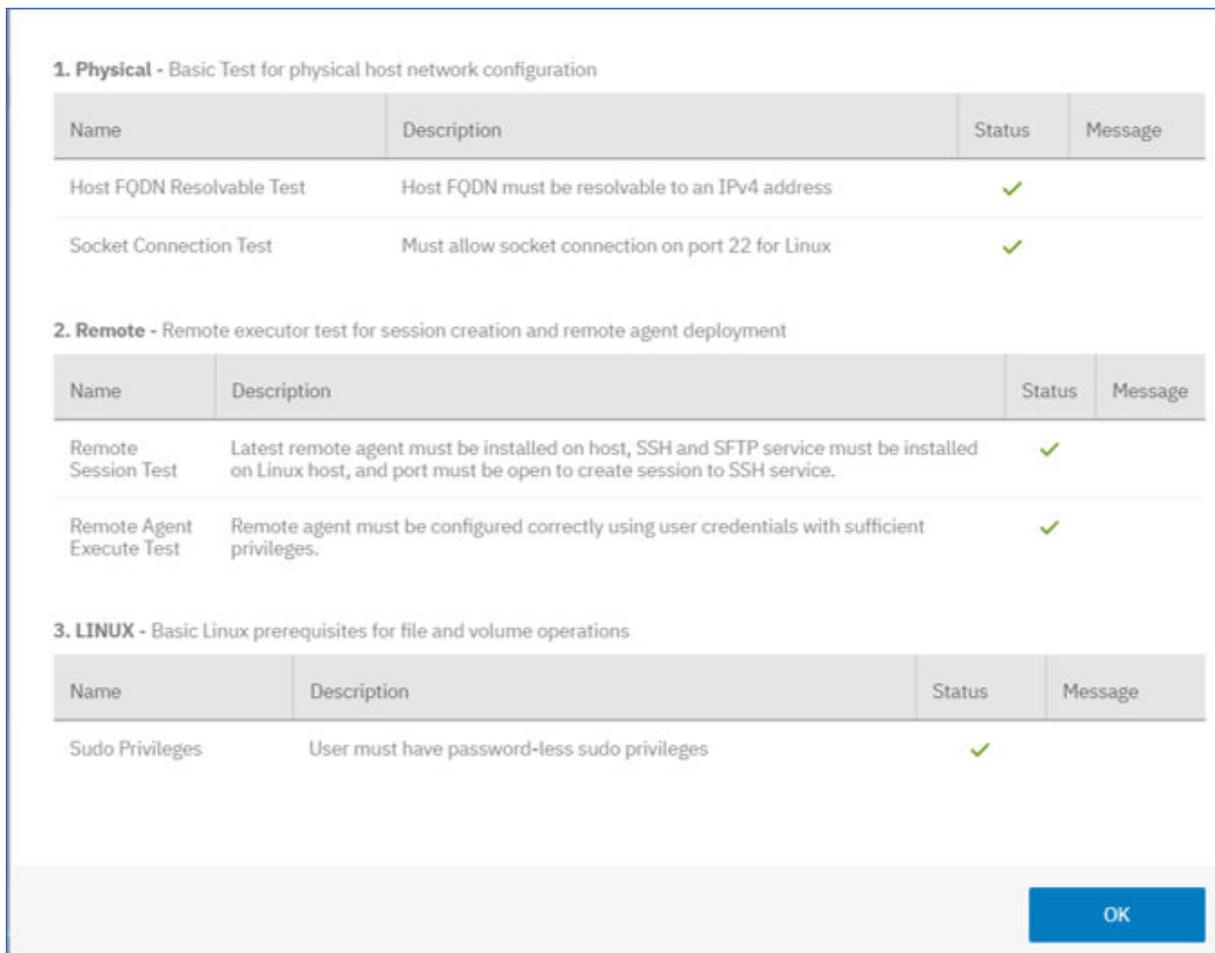
Para começar a proteger os bancos de dados MongoDB que estão catalogados na instância selecionada, aplique uma política de acordo de nível de serviço (ANS) à instância. Para obter instruções sobre como configurar uma política de ANS, consulte [Definindo uma política de ANS](#).

Testando a conexão MongoDB

Depois de incluir um servidor de aplicativos MongoDB, é possível testar a conexão. O teste verifica a comunicação entre o IBM Spectrum Protect Plus e o servidor MongoDB. Ele também verifica se a área de permissões sudo correta está disponível para o usuário que está executando o teste.

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > MongoDB**.
2. Na janela **MongoDB**, clique em **Gerenciar servidores de aplicativos** e selecione o endereço do host que você deseja testar.
É mostrada uma lista dos servidores de aplicativos MongoDB que estão disponíveis.
3. Clique em **Ações** e escolha **Testar** para iniciar os testes de verificação para conexões e configurações do sistema físicas e remotas.



1. Physical - Basic Test for physical host network configuration

Name	Description	Status	Message
Host FQDN Resolvable Test	Host FQDN must be resolvable to an IPv4 address	✓	
Socket Connection Test	Must allow socket connection on port 22 for Linux	✓	

2. Remote - Remote executor test for session creation and remote agent deployment

Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient privileges.	✓	

3. LINUX - Basic Linux prerequisites for file and volume operations

Name	Description	Status	Message
Sudo Privileges	User must have password-less sudo privileges	✓	

OK

O relatório de teste exibe uma lista que inclui testes para a configuração de rede do host físico e testes para a instalação do servidor remoto no host.

4. Clique em **OK** para fechar o relatório de teste. Se forem relatados problemas, corrija-os e execute novamente o teste para verificar as correções.

Fazendo backup de dados do MongoDB

Defina tarefas de backup regulares do MongoDB com opções para executar e criar cópias de backup para proteger seus dados. Para fazer backup de seus dados regularmente, defina uma tarefa de backup que inclua uma política de acordo de nível de serviço (ANS).

Antes de Iniciar

Durante a operação de backup inicial, o IBM Spectrum Protect Plus cria um novo volume vSnap e compartilhamento de NFS. Durante backups incrementais, o volume criado anteriormente é reutilizado. O agente do IBM Spectrum Protect Plus MongoDB monta o compartilhamento no servidor MongoDB no qual o backup é concluído.

Revise os seguintes pré-requisitos antes de criar uma definição de tarefa de backup:

- Inclua os servidores de aplicativos dos quais você deseja fazer backup. Para o procedimento, consulte [Incluindo um servidor de aplicativos MongoDB](#).
- Configure uma Política de SLA. Para o procedimento, consulte [Definindo uma tarefa de backup de Acordo de Nível de Serviço](#).
- Antes que um usuário do IBM Spectrum Protect Plus possa configurar operações de backup e restauração, as funções e grupos de recursos devem ser designados ao usuário. Conceda aos usuários acesso a recursos e operações de backup e restauração na área de janela **Contas**. Para obter mais informações, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#) e [“Roles para MongoDB” na página 197](#).
- Evite configurar backups de log para um único banco de dados MongoDB com muitas tarefas de backup. Se um único banco de dados MongoDB for incluído em várias definições de tarefa, um backup do log de uma tarefa pode truncar um log antes de ele ser submetido a backup pela próxima tarefa. Esta carga de trabalho pode causar falha nas tarefas de restauração point in time.
- A recuperação point in time não é suportada quando um ou mais arquivos de dados são incluídos no banco de dados no período entre o point-in-time escolhido e o horário em que a tarefa de backup anterior foi executada.

Restrição: Não execute tarefas de inventário ao mesmo tempo em que as tarefas de backup são planejadas.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > MongoDB**.
2. Selecione a caixa de seleção para a instância da qual você deseja fazer backup.

Em cada instância do MongoDB, os dados a serem submetidos a backup são listados como **ALL**. Cada instância na área de janela Instâncias é listada pelo nome da instância, versão e a política de ANS aplicada.

3. Clique em **Selecionar opções** para especificar o número de fluxos paralelos para a operação de backup e, em seguida, clique em **Salvar**. Ao selecionar um número apropriado de fluxos paralelos, é possível reduzir o tempo necessário para a tarefa de backup.

As opções salvas são usadas para todas as tarefas de backup para esta instância conforme selecionado.

4. Para executar a tarefa de backup com essas opções, clique no nome da instância, selecione a representação de banco de dados **ALL** e clique em **Executar**.

A tarefa de backup é iniciada e é possível visualizar os detalhes em **Tarefas e Operação > Tarefas em execução**.

Dica: O botão **Executar** é ativado apenas se uma política de SLA é aplicada à representação **ALL** dos bancos de dados.

5. Selecione a instância novamente e clique em **Selecionar uma política de SLA** para escolher uma política de SLA.
6. Salve a seleção de SLA.

Para definir um novo ANS ou editar uma política existente com taxas de retenção e frequência customizadas, selecione **Gerenciar proteção > Visão geral de política**. Na área de janela **Políticas de ANS**, clique em **Incluir política de ANS** e defina preferências de política.

O que Fazer Depois

Após o salvamento da política de ANS, é possível executar a política a qualquer momento, clicando em **Ações**, ao lado do nome da política e selecionando **Iniciar**. O status no log muda para mostrar que a tarefa de backup está no estado Running.

Para cancelar uma tarefa que está em execução, clique em **Ações** ao lado do nome da política e selecione **Cancelar**. Uma mensagem pergunta se você deseja manter os dados que já foram submetidos a backup. Escolha **Sim** para manter os dados submetidos a backup ou **Não** para descartar o backup.

Definindo uma tarefa de acordo de nível de serviço regular

Depois que as instâncias do MongoDB estiverem listadas, selecione e aplique uma política de ANS para começar a proteger seus dados.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > MongoDB**.
2. Selecione a instância do MongoDB para fazer backup de todos os dados nessa instância.

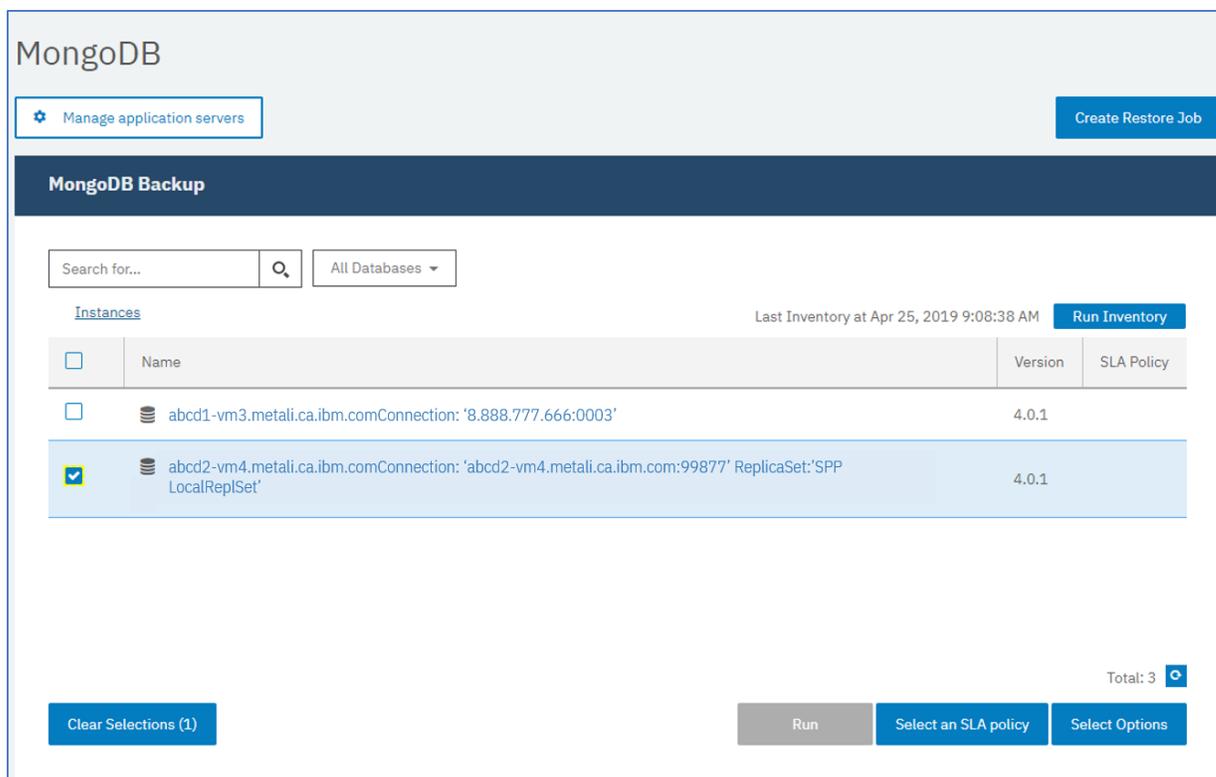


Figura 26. Área de Janela de Backup MongoDB mostrando instâncias

3. Clique em **Selecionar uma política de SLA** e escolha uma política de SLA. Salve sua opção.

As opções predefinidas são Ouro, Prata e Bronze, cada uma com diferentes frequências e taxas de retenção. Também é possível criar uma política de ANS customizada navegando para **Visão geral de política > Incluir política de ANS**.

4. Opcional: Para permitir que vários fluxos de backup reduzam o tempo gasto para fazer backup de bancos de dados grandes, clique em **Selecionar opções** e insira um número de fluxos paralelos. Salve suas mudanças.

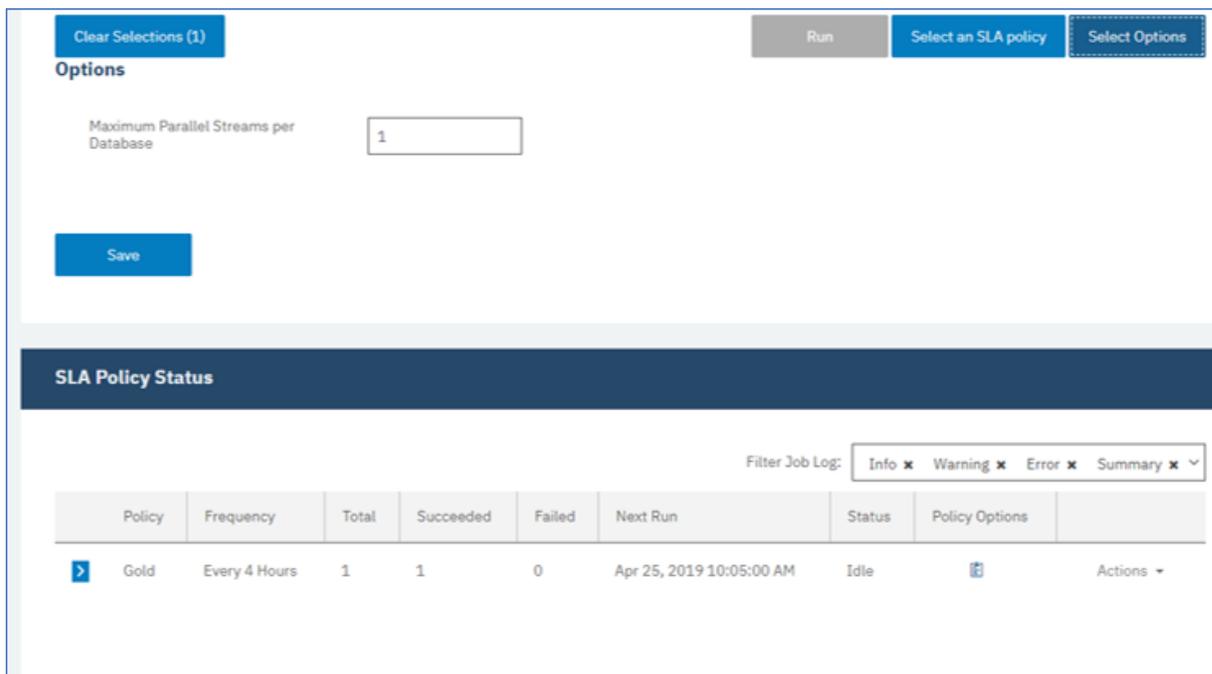


Figura 27. Opções de backup e status da política de SLA

- Configure a política de ANS clicando no ícone na coluna **Opções de política** da tabela **Status de política de ANS**.

Para obter informações adicionais sobre opções de configuração de ANS, consulte [“Definindo opções de configuração de ANS para seu backup”](#) na página 207.

- Para executar a política fora da tarefa planejada, selecione a instância. Clique no botão **Ações** e selecione **Iniciar**. O status muda para **Em execução** para seu ANS escolhido e é possível acompanhar o progresso da tarefa no log mostrado.

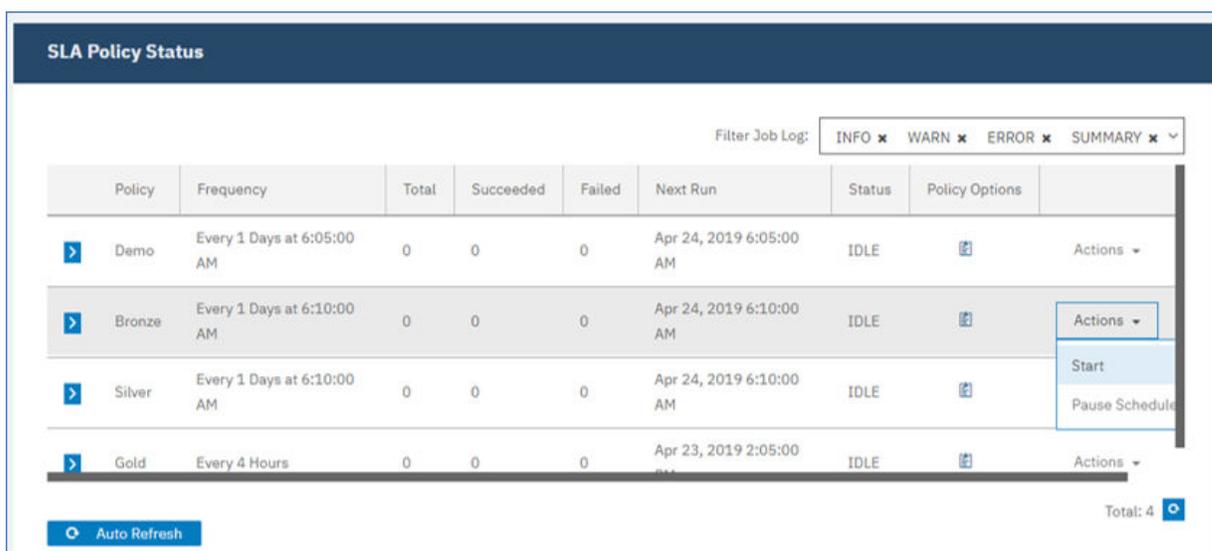


Figura 28. Políticas de SLA

O que Fazer Depois

Após o salvamento da política de ANS, é possível executar a política a qualquer momento, clicando em **Ações**, ao lado do nome da política e selecionando **Iniciar**. O status no log muda para mostrar que a tarefa de backup está no estado Running.

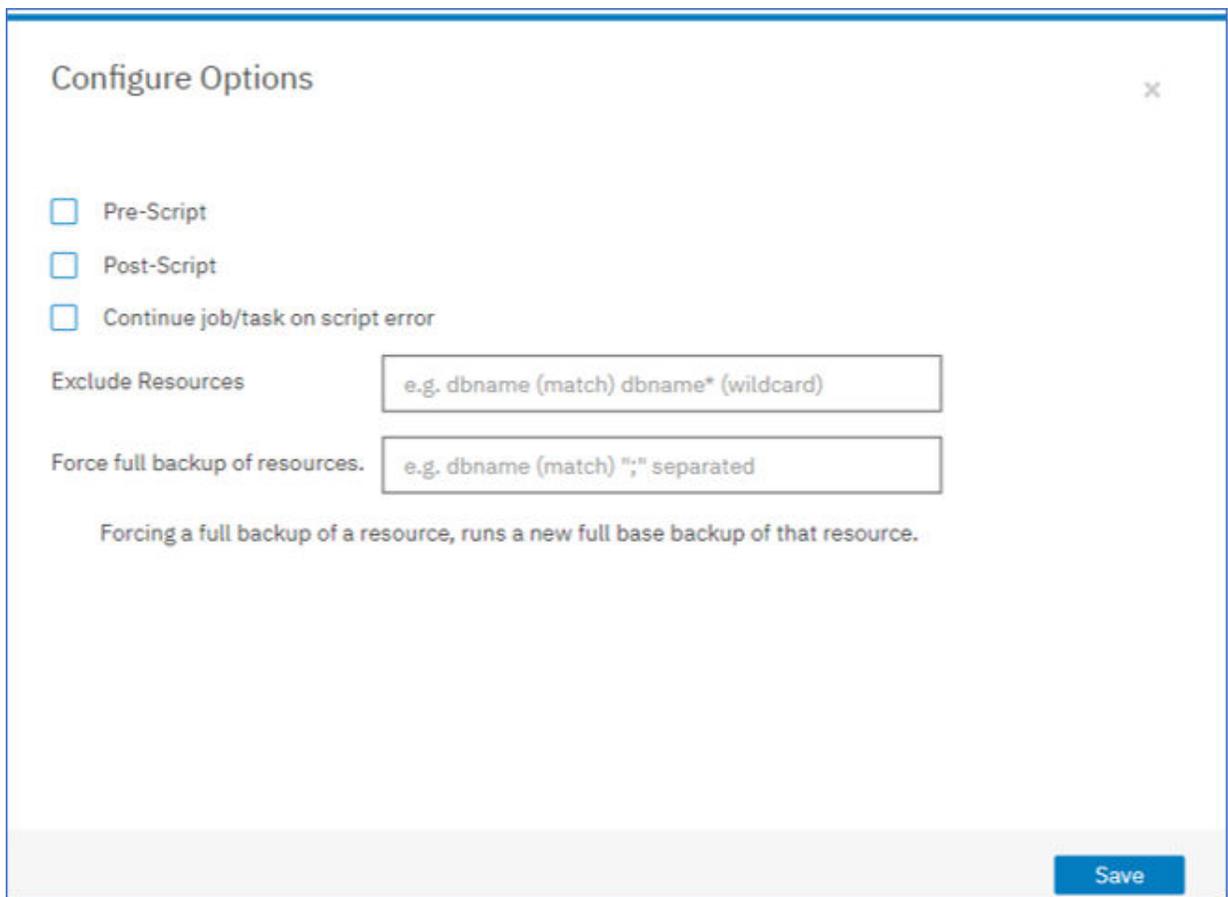
Para cancelar uma tarefa que está em execução, clique em **Ações** ao lado do nome da política e selecione **Cancelar**. Uma mensagem pergunta se você deseja manter os dados que já foram submetidos a backup. Escolha **Sim** para manter os dados submetidos a backup ou **Não** para descartar o backup.

Definindo opções de configuração de ANS para seu backup

Depois de configurar uma política de acordo de nível de serviço (ANS) para sua tarefa de backup, é possível escolher configurar opções extras para essa tarefa. As opções adicionais de ANS incluem executar scripts e forçar um backup de base completo.

Procedimento

1. Na coluna **Opções de política** da tabela **Status da política de ANS** para a tarefa que está sendo configurada, clique no ícone da área de transferência  para especificar opções de configuração adicionais.
Se a tarefa já estiver configurada, clique no ícone para editar a configuração.



Configure Options

Pre-Script

Post-Script

Continue job/task on script error

Exclude Resources

Force full backup of resources.

Forcing a full backup of a resource, runs a new full base backup of that resource.

Save

Figura 29. Especificando Opções de Configuração de SLA Adicionais

2. Clique em **Pré-script** e defina a configuração de pré-script escolhendo uma das seguintes opções:
 - Clique em **Usar servidor de script** e selecione um script transferido por upload do menu.
 - Não clique em **Usar Servidor de Script**. Selecione um servidor de aplicativos da lista para executar o script nesse local.
3. Clique em **Pós-script** e defina a configuração de PostScript escolhendo uma das seguintes opções:
 - Clique em **Usar servidor de script** e selecione um script transferido por upload do menu.
 - Não clique em **Usar Servidor de Script**. Selecione um servidor de aplicativos da lista para executar o script nesse local.

Os scripts e servidores de script são configurados na página **Configuração do sistema > Script**. Para obter informações adicionais sobre como trabalhar com scripts, consulte **Configurando scripts**.

4. Para continuar executando a tarefa quando o script associado à tarefa falhar, selecione **Continuar a tarefa durante erro do script**.

Se essa opção estiver selecionada, a operação de backup ou de restauração será tentada novamente após uma falha inicial e o status da tarefa de script será relatado como COMPLETED quando o script concluir o processamento com um código de retorno diferente de zero. Se esta opção não estiver selecionada, não haverá nova tentativa de backup ou restauração e o status da tarefa de script será relatado como COM FALHA.

5. Ignore **Excluir recursos** para opções de ANS do MongoDB, já que não é possível especificar recursos a serem excluídos. É feito backup de instâncias em vez de bancos de dados individuais.
6. Para criar um backup completo e novo de uma instância do MongoDB, selecione **Forçar backup completo de recursos**.

Um novo backup completo desse recurso é criado para substituir o backup existente desse recurso apenas para uma ocorrência. Depois disso, o recurso é submetido a backup incrementalmente como antes.

Restaurando Dados do MongoDB

Para restaurar dados, defina uma tarefa que restaure dados para o backup mais recente ou selecione uma cópia de backup anterior. Escolha restaurar dados para a instância original ou para uma instância alternativa em uma máquina diferente, criando uma cópia clonada. Defina e salve a tarefa de restauração para ser executada como uma operação ad hoc ou para ser executada regularmente como uma tarefa planejada.

Antes de Iniciar

Antes de criar uma tarefa de restauração para o MongoDB, assegure-se de que os requisitos a seguir tenham sido atendidos:

- Pelo menos uma tarefa de backup do MongoDB foi configurada e está sendo executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do MongoDB”](#) na página 203.
- Funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está configurando a tarefa de restauração. Para obter instruções sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297 e [“Roles para MongoDB”](#) na página 197.
- O espaço em disco suficiente é alocado no servidor de destino para a operação de restauração.
- Os volumes dedicados são alocados para cópia de arquivo.
- A mesma estrutura de diretório e layout estão disponíveis nos servidores de destino e de origem.
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Para operações de restauração para instâncias alternativas, o MongoDB deve estar no mesmo nível de versão nas máquinas de destino e host.

Para obter informações adicionais sobre requisitos de espaço, consulte [Pré-requisitos de espaço para proteção do MongoDB](#). Para obter informações adicionais sobre pré-requisitos e configuração, consulte [Pré-requisitos para o MongoDB](#).

Procedimento

Para definir uma tarefa de restauração do MongoDB, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > MongoDB > Criar tarefa de restauração** para abrir o assistente de Restauração de captura instantânea.

Dicas:

- Também é possível iniciar o assistente de Restauração de captura instantânea clicando em **Tarefas e Operações > Criar tarefa de restauração > MongoDB**.
 - Para obter um resumo em execução de suas seleções no assistente de Restauração de captura instantânea, mova o cursor para o ícone .
 - Se desejar ignorar as páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
- a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone Incluir na lista de restauração  ao lado do banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados. Para remover um item da origem da lista, clique no ícone Remover da lista de restauração  ao lado do item.
 - c) Clique em **Avançar** para continuar.
3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de restauração	<p>Selecione o tipo de tarefa de restauração a ser executada.</p> <p>On-Demand: captura instantânea Executa uma operação de restauração única a partir de um backup de captura instantânea.</p> <p>On-Demand: momento Executa uma operação de restauração única a partir de um backup de momento específico.</p> <p>Recorrente Executa operações planejadas de restauração de dados a partir dos pontos de restauração mais recentes.</p>
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual fazer a restauração:</p> <p>Site Restaura dados de um site que está associado ao servidor de armazenamento de backup.</p> <p>Transferência de nuvem Restaura dados que estão armazenados no armazenamento em nuvem.</p> <p>Transferência de repositório Restaura dados que estão armazenados no servidor do repositório.</p> <p>Archive de nuvem Restaura dados que estão arquivados no armazenamento em nuvem.</p> <p>Archive de repositório Restaura dados que estão arquivados no servidor do repositório.</p>
Selecionar uma Posição	<p>Se estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo Restaura dados do servidor vSnap de demonstração que é configurado para fins de teste.</p>

Opção	Descrição
	<p>Primário Restaura dados do servidor vSnap que é o destino de backup primário.</p> <p>Secundário Restaura dados do servidor vSnap que é o destino de backup secundário.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, não será necessário fazer uma seleção porque o local já está selecionado.</p>
Seletor de Data	Para operações de restauração on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo de datas.
Ponto de Restauração	Para operações de restauração sob demanda, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de data selecionado.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Selecione essa caixa para especificar um servidor vSnap alternativo quando você estiver restaurando um ponto de restauração específico de um recurso em nuvem ou servidor do repositório e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido para um recurso em nuvem ou um servidor de repositório, um servidor vSnap é usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir o carregamento no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway para a operação de restauração.</p>

4. Na página **Configurar destino**, selecione **Restaurar para a instância original** para restaurar para o servidor original ou **Restaurar para uma instância alternativa** para restaurar para um local diferente, que pode ser selecionado nos locais listados.

Para obter informações adicionais sobre como restaurar dados para a instância original, consulte [Restaurando para a instância original](#). Para obter informações adicionais sobre como restaurar seus dados para uma instância alternativa, consulte [Restaurando para uma instância alternativa](#).

5. Na página **Método de restauração**, escolha o tipo de operação de restauração e clique em **Avançar** para continuar.

- **Teste:** Nesse modo, o agente cria um banco de dados usando os arquivos de dados diretamente do repositório do vSnap. Esta opção está disponível apenas quando você está restaurando dados para uma instância alternativa. Membros de conjuntos de réplicas não serão reconfigurados após o início do servidor MongoDB. O servidor é iniciado como um conjunto de réplicas de nó único.
- **Produção:** nesse modo, o servidor de aplicativos MongoDB copia primeiro os arquivos do repositório do vSnap para o host de destino. Em seguida, os dados copiados são usados para iniciar o banco de dados. As instâncias do MongoDB que são membros de um conjunto de réplicas não são iniciadas durante uma operação de restauração de produção. Esta ação impede que os dados sejam sobrescritos durante a conexão com o conjunto de réplicas.
- **Acesso instantâneo:** Nesse modo, nenhuma ação adicional é executada após o IBM Spectrum Protect Plus montar o compartilhamento. Use os dados para recuperação customizada a partir dos arquivos no repositório do vSnap.

Para o modo de teste ou de produção, é possível, opcionalmente, inserir um novo nome para o banco de dados restaurado.

Para o modo de produção, também é possível especificar uma nova pasta para o banco de dados restaurado expandindo o banco de dados e inserindo um novo nome de pasta.

6. Opcional: Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Na seção **Opções de recuperação**, a opção **Recuperar até o término de backup** para MongoDB é selecionada por padrão. Esta opção recupera os dados selecionados para o estado em que estava no momento em que o backup foi criado. A operação de recuperação faz uso dos arquivos de log que estão incluídos no backup do MongoDB.

Opções do Aplicativo

Configure as opções do aplicativo:

Sobrescrever banco de dados

Ative esta opção para permitir que a tarefa de restauração sobrescreva o banco de dados selecionado. Se essa opção não estiver selecionada, a tarefa de restauração falhará quando os dados com o mesmo nome forem localizados durante o processo de restauração.



Atenção: Assegure-se de que nenhum outro dado compartilhe o mesmo diretório de banco de dados local que os dados originais ou os dados serão sobrescritos.

Máximo de Fluxos Paralelo por Banco de Dados

Configure o número máximo de fluxos de dados paralelos a partir do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Múltiplos bancos de dados ainda poderão ser restaurados em paralelo se o valor da opção for configurado como 1. Múltiplos fluxos paralelos podem acelerar as operações de restauração, mas o consumo alto de largura da banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas quando você estiver restaurando um banco de dados MongoDB para seu local original usando seu nome de banco de dados original.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Essa opção é selecionada, por padrão, para limpar automaticamente os recursos alocados como parte de uma operação de restauração se a recuperação falhar.

Permitir sobrescrição de sessão

Selecione esta opção para substituir os bancos de dados existentes com o mesmo nome durante uma operação de restauração. Durante uma operação de restauração instantânea de disco, o banco de dados existente é encerrado e sobrescrito e, em seguida, o banco de dados recuperado é reiniciado. Se essa opção não estiver selecionada e um banco de dados com o mesmo nome for encontrado, a operação de restauração falhará com um erro.

Continuar com restaurações de outros bancos de dados selecionados, mesmo se um falhar

Se um banco de dados na instância não for restaurado com êxito, a operação de restauração continuará para todos os outros dados que estão sendo restaurados. Quando esta opção não estiver selecionada, a tarefa de restauração será parada quando a recuperação de um recurso falhar.

Prefixo do ponto de montagem

Para operações de restauração de **Acesso instantâneo**, especifique um prefixo de ponto de montagem para o caminho em que a montagem deve ser direcionada.

7. Opcional: Na página **Aplicar scripts**, especifique os scripts que podem ser executados antes ou depois de uma tarefa ser executada. Os scripts de lote e PowerShell são suportados em sistemas operacionais Windows, enquanto os shell scripts são suportados em sistemas operacionais Linux .

Pré-Script

Marque essa caixa de seleção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pré-script será executado. Para selecionar um servidor de aplicativos, limpe a caixa de seleção **Usar servidor de script**. Para configurar scripts e servidores de script, clique em **Configuração do sistema > Script**.

Pós-script

Selecione essa opção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pós-script será executado. Para selecionar um servidor de aplicativos,

limpe a caixa de seleção **Usar servidor de script**. Para configurar scripts e servidores de script, clique na página **Configuração do sistema > Script**.

Continuar job/tarefa no erro de script

Selecione essa opção para continuar executando a tarefa quando o script que estiver associado à tarefa falhar. Quando essa opção estiver ativada, no caso de um script concluir o processamento com um código de retorno diferente de zero, a tarefa de backup ou restauração continuará a ser executada e o status da tarefa de pré-script será relatado como COMPLETED. Se um pós-script concluir o processamento com um código de retorno diferente de zero, o O status da tarefa de pós-script será relatado como COMPLETED. Quando essa opção não é selecionada, a tarefa de backup ou restauração não é executada e a tarefa de pré-script ou pós-script é relatada como FAILED.

Clique em **Avançar** para continuar.

8. Na página **Planejamento**, clique em **Avançar** para iniciar tarefas sob demanda depois de concluir o assistente de Restauração de captura instantânea. Para tarefas recorrentes, insira um nome para o planejamento de tarefa e especifique com que frequência e quando iniciar a tarefa de restauração.
9. Na página **Revisar**, revise as configurações da tarefa de restauração.



Atenção: Revise as opções selecionadas antes de continuar em **Enviar** porque os dados serão sobrescritos quando a opção de aplicativo **Sobrescrever dados existentes** for selecionada. É possível cancelar uma tarefa de restauração quando ela estiver em andamento, mas se a opção **Sobrescrever dados existentes** for selecionada, os dados serão sobrescritos mesmo se você cancelar a tarefa.

10. Para continuar com a tarefa, clique em **Enviar**. Para cancelar a tarefa, navegue para **Tarefas e operações** e clique na guia **Planejamento**. Localize a tarefa de restauração que deseja cancelar. Clique em **Ações** e selecione **Cancelar**.

Resultados

Poucos minutos depois de selecionar **Restaurar**, a tarefa **onDemandRestore** é incluída na área de janela **Tarefas e operações > Tarefas em execução**. Clique no registro para mostrar os detalhes passo a passo da operação. Também é possível fazer download do arquivo de log compactado clicando em **Download.zip**. Para quaisquer outras tarefas, clique nas guias **Tarefas em execução** ou **Histórico da tarefa** e clique na tarefa para exibir seus detalhes.

O endereço IP e a porta para o servidor restaurado podem ser localizados no arquivo de log para a operação de restauração. Navegue para **Tarefas e operações > Tarefas em execução** para localizar os logs para sua operação de restauração.

Para obter informações sobre como restaurar dados para a instância original, consulte [Restaurando para a instância original](#). Para obter informações sobre como restaurar seus dados para uma instância alternativa, consulte [Restaurando para uma instância alternativa](#).

Restaurando dados do MongoDB para a instância original

É possível restaurar uma instância do MongoDB para o host original e escolher entre a restauração para o backup mais recente ou para uma versão de backup de banco de dados do MongoDB anterior. Ao restaurar dados para sua instância original, não é possível renomeá-los. Essa opção de restauração executa uma restauração completa da produção de dados, e os dados existentes serão sobrescritos no site de destino se a opção de aplicativo **Sobrescrever bancos de dados existentes** estiver selecionada.

Antes de Iniciar

Antes de criar uma tarefa de restauração para o MongoDB, assegure-se de que os requisitos a seguir tenham sido atendidos:

- Pelo menos uma tarefa de backup do MongoDB foi configurada e está sendo executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do MongoDB”](#) na página 203.

- Funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está configurando a tarefa de restauração. Para obter instruções sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#) e [“Roles para MongoDB” na página 197](#).
- O espaço em disco suficiente é alocado no servidor de destino para a operação de restauração.
- Os volumes dedicados são alocados para cópia de arquivo.
- A mesma estrutura de diretório e layout estão disponíveis nos servidores de destino e de origem.
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Para obter informações adicionais sobre requisitos de espaço, consulte [Pré-requisitos de espaço para proteção do MongoDB](#). Para obter informações adicionais sobre pré-requisitos e configuração, consulte [Pré-requisitos para o MongoDB](#).

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > MongoDB > Criar tarefa de restauração** para abrir o assistente de Restauração de captura instantânea.

Dicas:

- Também é possível iniciar o assistente de Restauração de captura instantânea clicando em **Tarefas e Operações > Criar tarefa de restauração > MongoDB**.
 - Para obter um resumo em execução de suas seleções no assistente de Restauração de captura instantânea, mova o cursor para o ícone .
 - Se desejar ignorar as páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone Incluir na lista de restauração  ao lado do banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados. Para remover um item da origem da lista, clique no ícone Remover da lista de restauração  ao lado do item.
 - c) Clique em **Avançar** para continuar.

3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de restauração	<p>Selecione o tipo de tarefa de restauração a ser executada.</p> <p>On-Demand: captura instantânea Executa uma operação de restauração única a partir de um backup de captura instantânea.</p> <p>On-Demand: momento Executa uma operação de restauração única a partir de um backup de momento específico.</p> <p>Recorrente Executa operações planejadas de restauração de dados a partir dos pontos de restauração mais recentes.</p>

Opção	Descrição
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual fazer a restauração:</p> <p>Site Restaura dados de um site que está associado ao servidor de armazenamento de backup.</p> <p>Transferência de nuvem Restaura dados que estão armazenados no armazenamento em nuvem.</p> <p>Transferência de repositório Restaura dados que estão armazenados no servidor do repositório.</p> <p>Archive de nuvem Restaura dados que estão arquivados no armazenamento em nuvem.</p> <p>Archive de repositório Restaura dados que estão arquivados no servidor do repositório.</p>
Selecionar uma Posição	<p>Se estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo Restaura dados do servidor vSnap de demonstração que é configurado para fins de teste.</p> <p>Primário Restaura dados do servidor vSnap que é o destino de backup primário.</p> <p>Secundário Restaura dados do servidor vSnap que é o destino de backup secundário.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, não será necessário fazer uma seleção porque o local já está selecionado.</p>
Seletor de Data	<p>Para operações de restauração on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo de datas.</p>
Ponto de Restauração	<p>Para operações de restauração sob demanda, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de data selecionado.</p>
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Selecione essa caixa para especificar um servidor vSnap alternativo quando você estiver restaurando um ponto de restauração específico de um recurso em nuvem ou servidor do repositório e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido para um recurso em nuvem ou um servidor de repositório, um servidor vSnap é usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir o carregamento no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway para a operação de restauração.</p>

4. Na página "Configurar destino", escolha **Restaurar para a instância original** e clique em **Avançar**.
5. Na página **Método de restauração**, escolha o tipo de operação de restauração e clique em **Avançar** para continuar.

- **Produção**

Para recuperar uma instância inteira para a instância original, o método preferencial é escolher essa opção com a opção de sobrescrição de aplicativo. As instâncias do MongoDB que são membros de um conjunto de réplicas não são iniciadas durante uma operação de restauração de

produção. Esta ação impede que os dados sejam sobrescritos durante a conexão com o conjunto de réplicas.

- **Teste**

Escolha essa opção para restaurar dados para o mesmo servidor, mas usando uma porta diferente.

- **Acesso Instantâneo**

Escolha essa opção para montar o backup para o servidor de aplicativos sem restaurar ou sobrescrever os dados.

Clique em **Avançar** para continuar.

Para o modo de teste ou de produção, é possível, opcionalmente, inserir um novo nome para o banco de dados restaurado.

Para o modo de produção, também é possível especificar uma nova pasta para o banco de dados restaurado expandindo o banco de dados e inserindo um novo nome de pasta.

6. Opcional: Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Na seção **Opções de recuperação**, a opção **Recuperar até o término de backup** para MongoDB é selecionada por padrão. Esta opção recupera os dados selecionados para o estado em que estava no momento em que o backup foi criado. A operação de recuperação faz uso dos arquivos de log que estão incluídos no backup do MongoDB.

Opções do Aplicativo

Configure as opções do aplicativo:

Sobrescrever banco de dados

Ative esta opção para permitir que a tarefa de restauração sobrescreva o banco de dados selecionado. Se essa opção não estiver selecionada, a tarefa de restauração falhará quando os dados com o mesmo nome forem localizados durante o processo de restauração.



Atenção: Assegure-se de que nenhum outro dado compartilhe o mesmo diretório de banco de dados local que os dados originais ou os dados serão sobrescritos.

Máximo de Fluxos Paralelo por Banco de Dados

Configure o número máximo de fluxos de dados paralelos a partir do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Múltiplos bancos de dados ainda poderão ser restaurados em paralelo se o valor da opção for configurado como 1. Múltiplos fluxos paralelos podem acelerar as operações de restauração, mas o consumo alto de largura da banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas quando você estiver restaurando um banco de dados MongoDB para seu local original usando seu nome de banco de dados original.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Essa opção é selecionada, por padrão, para limpar automaticamente os recursos alocados como parte de uma operação de restauração se a recuperação falhar.

Permitir sobrescrição de sessão

Selecione esta opção para substituir os bancos de dados existentes com o mesmo nome durante uma operação de restauração. Durante uma operação de restauração instantânea de disco, o banco de dados existente é encerrado e sobrescrito e, em seguida, o banco de dados recuperado é reiniciado. Se essa opção não estiver selecionada e um banco de dados com o mesmo nome for encontrado, a operação de restauração falhará com um erro.

Continuar com restaurações de outros bancos de dados selecionados, mesmo se um falhar

Se um banco de dados na instância não for restaurado com êxito, a operação de restauração continuará para todos os outros dados que estão sendo restaurados. Quando esta opção não

estiver selecionada, a tarefa de restauração será parada quando a recuperação de um recurso falhar.

Prefixo do ponto de montagem

Para operações de restauração de **Acesso instantâneo**, especifique um prefixo de ponto de montagem para o caminho em que a montagem deve ser direcionada.

7. Opcional: Na página **Aplicar scripts**, especifique os scripts que podem ser executados antes ou depois de uma tarefa ser executada. Os scripts de lote e PowerShell são suportados em sistemas operacionais Windows, enquanto os shell scripts são suportados em sistemas operacionais Linux .

Pré-Script

Marque essa caixa de seleção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pré-script será executado. Para selecionar um servidor de aplicativos, limpe a caixa de seleção **Usar servidor de script**. Para configurar scripts e servidores de script, clique em **Configuração do sistema > Script**.

Pós-script

Selecione essa opção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pós-script será executado. Para selecionar um servidor de aplicativos, limpe a caixa de seleção **Usar servidor de script**. Para configurar scripts e servidores de script, clique na página **Configuração do sistema > Script**.

Continuar job/tarefa no erro de script

Selecione essa opção para continuar executando a tarefa quando o script que estiver associado à tarefa falhar. Quando essa opção estiver ativada, no caso de um script concluir o processamento com um código de retorno diferente de zero, a tarefa de backup ou restauração continuará a ser executada e o status da tarefa de pré-script será relatado como COMPLETED. Se um pós-script concluir o processamento com um código de retorno diferente de zero, o O status da tarefa de pós-script será relatado como COMPLETED. Quando essa opção não é selecionada, a tarefa de backup ou restauração não é executada e a tarefa de pré-script ou pós-script é relatada como FAILED.

Clique em **Avançar** para continuar.

8. Na página **Planejamento**, clique em **Avançar** para iniciar tarefas sob demanda depois de concluir o assistente de Restauração de captura instantânea. Para tarefas recorrentes, insira um nome para o planejamento de tarefa e especifique com que frequência e quando iniciar a tarefa de restauração.
9. Na página **Revisar**, revise as configurações da tarefa de restauração.



Atenção: Revise as opções selecionadas antes de continuar em **Enviar** porque os dados serão sobrescritos quando a opção de aplicativo **Sobrescrever dados existentes** for selecionada. É possível cancelar uma tarefa de restauração quando ela estiver em andamento, mas se a opção **Sobrescrever dados existentes** for selecionada, os dados serão sobrescritos mesmo se você cancelar a tarefa.

10. Para continuar com a tarefa, clique em **Enviar**. Para cancelar a tarefa, navegue para **Tarefas e operações** e clique na guia **Planejamento**. Localize a tarefa de restauração que deseja cancelar. Clique em **Ações** e selecione **Cancelar** .

Restaurando dados do MongoDB para uma instância alternativa

É possível selecionar um backup de banco de dados do MongoDB e restaurá-lo para um host alternativo. Também é possível escolher restaurar um banco de dados para um repositório do vSnap diferente ou é possível renomear o banco de dados. Este processo cria uma cópia exata da instância em um host diferente.

Antes de Iniciar

Antes de criar uma tarefa de restauração para o MongoDB, assegure-se de que os requisitos a seguir tenham sido atendidos:

- Pelo menos uma tarefa de backup do MongoDB foi configurada e está sendo executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do MongoDB”](#) na página 203.
- Funções e grupos de recursos do IBM Spectrum Protect Plus são designados ao usuário que está configurando a tarefa de restauração. Para obter instruções sobre como designar funções, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297 e [“Roles para MongoDB”](#) na página 197.
- O espaço em disco suficiente é alocado no servidor de destino para a operação de restauração.
- Os volumes dedicados são alocados para cópia de arquivo.
- A mesma estrutura de diretório e layout estão disponíveis nos servidores de destino e de origem.
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Para operações de restauração para instâncias alternativas, o MongoDB deve estar no mesmo nível de versão nas máquinas de destino e host.

Para obter informações adicionais sobre requisitos de espaço, consulte [Pré-requisitos de espaço para proteção do MongoDB](#). Para obter informações adicionais sobre pré-requisitos e configuração, consulte [Pré-requisitos para o MongoDB](#).

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > MongoDB > Criar tarefa de restauração** para abrir o assistente de Restauração de captura instantânea.

Dicas:

- Também é possível iniciar o assistente de Restauração de captura instantânea clicando em **Tarefas e Operações > Criar tarefa de restauração > MongoDB**.
 - Para obter um resumo em execução de suas seleções no assistente de Restauração de captura instantânea, mova o cursor para o ícone .
 - Se desejar ignorar as páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone Incluir na lista de restauração  ao lado do banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados.
Para remover um item da origem da lista, clique no ícone Remover da lista de restauração  ao lado do item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Tipo de restauração	Selecione o tipo de tarefa de restauração a ser executada. On-Demand: captura instantânea Executa uma operação de restauração única a partir de um backup de captura instantânea.

Opção	Descrição
	<p>On-Demand: momento Executa uma operação de restauração única a partir de um backup de momento específico.</p> <p>Recorrente Executa operações planejadas de restauração de dados a partir dos pontos de restauração mais recentes.</p>
Tipo de local da restauração	<p>Selecione um tipo de local a partir do qual fazer a restauração:</p> <p>Site Restaura dados de um site que está associado ao servidor de armazenamento de backup.</p> <p>Transferência de nuvem Restaura dados que estão armazenados no armazenamento em nuvem.</p> <p>Transferência de repositório Restaura dados que estão armazenados no servidor do repositório.</p> <p>Archive de nuvem Restaura dados que estão arquivados no armazenamento em nuvem.</p> <p>Archive de repositório Restaura dados que estão arquivados no servidor do repositório.</p>
Selecionar uma Posição	<p>Se estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo Restaura dados do servidor vSnap de demonstração que é configurado para fins de teste.</p> <p>Primário Restaura dados do servidor vSnap que é o destino de backup primário.</p> <p>Secundário Restaura dados do servidor vSnap que é o destino de backup secundário.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, não será necessário fazer uma seleção porque o local já está selecionado.</p>
Seletor de Data	<p>Para operações de restauração on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo de datas.</p>
Ponto de Restauração	<p>Para operações de restauração sob demanda, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de data selecionado.</p>
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Selecione essa caixa para especificar um servidor vSnap alternativo quando você estiver restaurando um ponto de restauração específico de um recurso em nuvem ou servidor do repositório e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido para um recurso em nuvem ou um servidor de repositório, um servidor vSnap é usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir o carregamento no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway para a operação de restauração.</p>

4. Na página **Configurar destino**, escolha **Restaurar para uma instância alternativa** e selecione a instância de destino para a qual você deseja restaurar os dados.

A instância original não é selecionável porque não é possível sobrescrever os dados originais quando você seleciona **Restaurar para instância alternativa**. Também não é possível selecionar instâncias em diferentes níveis de versões ou instâncias no mesmo host que a instância original.

Clique em **Avançar** para continuar.

5. Na página **Método de restauração**, escolha o tipo de operação de restauração e clique em **Avançar** para continuar.
 - **Teste**: Nesse modo, o agente cria um banco de dados usando os arquivos de dados diretamente do repositório do vSnap. Esta opção está disponível apenas quando você está restaurando dados para uma instância alternativa. Membros de conjuntos de réplicas não serão reconfigurados após o início do servidor MongoDB. O servidor é iniciado como um conjunto de réplicas de nó único.
 - **Produção**: nesse modo, o servidor de aplicativos MongoDB copia primeiro os arquivos do repositório do vSnap para o host de destino. Em seguida, os dados copiados são usados para iniciar o banco de dados. As instâncias do MongoDB que são membros de um conjunto de réplicas não são iniciadas durante uma operação de restauração de produção. Esta ação impede que os dados sejam sobrescritos durante a conexão com o conjunto de réplicas.
 - **Acesso instantâneo**: Nesse modo, nenhuma ação adicional é executada após o IBM Spectrum Protect Plus montar o compartilhamento. Use os dados para recuperação customizada a partir dos arquivos no repositório do vSnap.

Para o modo de teste ou de produção, é possível, opcionalmente, inserir um novo nome para o banco de dados restaurado.

Para o modo de produção, também é possível especificar uma nova pasta para o banco de dados restaurado expandindo o banco de dados e inserindo um novo nome de pasta.

6. Opcional: Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Na seção **Opções de recuperação**, a opção **Recuperar até o término de backup** para MongoDB é selecionada por padrão. Esta opção recupera os dados selecionados para o estado em que estava no momento em que o backup foi criado. A operação de recuperação faz uso dos arquivos de log que estão incluídos no backup do MongoDB.

Opções do Aplicativo

Configure as opções do aplicativo:

Sobrescrever banco de dados

Ative esta opção para permitir que a tarefa de restauração sobrescreva o banco de dados selecionado. Se essa opção não estiver selecionada, a tarefa de restauração falhará quando os dados com o mesmo nome forem localizados durante o processo de restauração.



Atenção: Assegure-se de que nenhum outro dado compartilhe o mesmo diretório de banco de dados local que os dados originais ou os dados serão sobrescritos.

Máximo de Fluxos Paralelo por Banco de Dados

Configure o número máximo de fluxos de dados paralelos a partir do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Múltiplos bancos de dados ainda poderão ser restaurados em paralelo se o valor da opção for configurado como 1. Múltiplos fluxos paralelos podem acelerar as operações de restauração, mas o consumo alto de largura da banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas quando você estiver restaurando um banco de dados MongoDB para seu local original usando seu nome de banco de dados original.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Essa opção é selecionada, por padrão, para limpar automaticamente os recursos alocados como parte de uma operação de restauração se a recuperação falhar.

Permitir sobrescrição de sessão

Selecione esta opção para substituir os bancos de dados existentes com o mesmo nome durante uma operação de restauração. Durante uma operação de restauração instantânea de disco, o banco de dados existente é encerrado e sobrescrito e, em seguida, o banco de dados recuperado é reiniciado. Se essa opção não estiver selecionada e um banco de dados com o mesmo nome for encontrado, a operação de restauração falhará com um erro.

Continuar com restaurações de outros bancos de dados selecionados, mesmo se um falhar

Se um banco de dados na instância não for restaurado com êxito, a operação de restauração continuará para todos os outros dados que estão sendo restaurados. Quando esta opção não estiver selecionada, a tarefa de restauração será parada quando a recuperação de um recurso falhar.

Prefixo do ponto de montagem

Para operações de restauração de **Acesso instantâneo**, especifique um prefixo de ponto de montagem para o caminho em que a montagem deve ser direcionada.

7. Opcional: Na página **Aplicar scripts**, especifique os scripts que podem ser executados antes ou depois de uma tarefa ser executada. Os scripts de lote e PowerShell são suportados em sistemas operacionais Windows, enquanto os shell scripts são suportados em sistemas operacionais Linux .

Pré-Script

Marque essa caixa de seleção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pré-script será executado. Para selecionar um servidor de aplicativos, limpe a caixa de seleção **Usar servidor de script**. Para configurar scripts e servidores de script, clique em **Configuração do sistema > Script**.

Pós-script

Selecione essa opção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pós-script será executado. Para selecionar um servidor de aplicativos, limpe a caixa de seleção **Usar servidor de script**. Para configurar scripts e servidores de script, clique na página **Configuração do sistema > Script**.

Continuar job/tarefa no erro de script

Selecione essa opção para continuar executando a tarefa quando o script que estiver associado à tarefa falhar. Quando essa opção estiver ativada, no caso de um script concluir o processamento com um código de retorno diferente de zero, a tarefa de backup ou restauração continuará a ser executada e o status da tarefa de pré-script será relatado como COMPLETED. Se um pós-script concluir o processamento com um código de retorno diferente de zero, o status da tarefa de pós-script será relatado como COMPLETED. Quando essa opção não é selecionada, a tarefa de backup ou restauração não é executada e a tarefa de pré-script ou pós-script é relatada como FAILED.

Clique em **Avançar** para continuar.

8. Na página **Planejamento**, clique em **Avançar** para iniciar tarefas sob demanda depois de concluir o assistente de Restauração de captura instantânea. Para tarefas recorrentes, insira um nome para o planejamento de tarefa e especifique com que frequência e quando iniciar a tarefa de restauração.
9. Na página **Revisar**, revise as configurações da tarefa de restauração.



Atenção: Revise as opções selecionadas antes de continuar em **Enviar** porque os dados serão sobrescritos quando a opção de aplicativo **Sobrescrever dados existentes** for selecionada. É possível cancelar uma tarefa de restauração quando ela estiver em andamento, mas se a opção **Sobrescrever dados existentes** for selecionada, os dados serão sobrescritos mesmo se você cancelar a tarefa.

10. Para continuar com a tarefa, clique em **Enviar**. Para cancelar a tarefa, navegue para **Tarefas e operações** e clique na guia **Planejamento**. Localize a tarefa de restauração que deseja cancelar. Clique em **Ações** e selecione **Cancelar** .

Usando uma operação de restauração granular para MongoDB

É possível restaurar bancos de dados ou coleções específicas do MongoDB usando uma operação de restauração granular. Para uma operação de restauração granular, primeiro execute uma tarefa de restauração de teste e, em seguida, execute os comandos adequados do MongoDB.

Antes de Iniciar

Se a autenticação estiver ativada, deve-se fornecer credenciais para os usuários para que eles possam corrigir as permissões na instância na operação de restauração de teste.

Sobre Esta Tarefa

A operação de restauração granular para o MongoDB é baseada em uma tarefa de restauração de modo de teste. Ao executar a tarefa de restauração de teste no IBM Spectrum Protect Plus executar os comandos **mongodump** e **mongoexport** no servidor MongoDB, é possível acessar bancos de dados ou coleções individuais a partir da origem de recuperação.

Use este procedimento para concluir uma das tarefas a seguir:

- Restaurar qualquer número de bancos de dados usando os comandos **mongodump** e **mongoexport** para os bancos de dados necessários.
- Restaurar qualquer número de coleções usando os comandos **mongodump** e **mongoexport** para as coleções necessárias.

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > MongoDB**.
2. Clique em **Criar tarefa de restauração** para abrir o assistente de restauração. O MongoDB é selecionado automaticamente.
3. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone Incluir na lista de restauração  ao lado do banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados.

Para remover um item da origem da lista, clique no ícone Remover da lista de restauração  ao lado do item.
 - c) Clique em **Avançar** para continuar.
4. Na página **Configurar destino**, escolha **Restaurar para instância alternativa** e selecione a instância de destino para a qual você deseja restaurar os dados.

Não é possível selecionar a instância original, uma vez que não é possível sobrescrever os dados originais ao selecionar **Restaurar para instância alternativa**. Instâncias em níveis de versões diferentes não podem ser selecionadas. Outras instâncias no mesmo host que a instância original também não podem ser selecionadas.

Clique em **Avançar** para continuar.
5. Na página **Método de restauração**, selecione **Testar** e clique em **Avançar** para continuar com o processo de restauração de teste.
6. Prossiga pelas páginas do assistente de restauração e selecione as opções necessárias.
7. Na página **Revisar**, revise as configurações da tarefa de restauração.



Atenção: Revise as opções selecionadas antes de continuar em **Enviar** porque os dados serão sobrescritos quando a opção de aplicativo **Sobrescrever dados existentes** for selecionada. É possível cancelar uma tarefa de restauração quando ela estiver em andamento, mas se a

opção **Sobrescrever dados existentes** for selecionada, os dados serão sobrescritos mesmo se você cancelar a tarefa.

8. Efetue logon no servidor MongoDB para o qual a tarefa de restauração de teste é direcionada.
9. Execute o comando do sistema `ps -ef | grep mongod` do MongoDB para encontrar o local da instância do MongoDB de recuperação temporária.
10. Execute o comando `mongodump` do MongoDB para criar um arquivo dump de qualquer banco de dados ou coleta específica.

Use o comando apropriado. O primeiro comando é para um banco de dados e o segundo comando é para uma coleção:

```
mongodump --host <hostname> --port <port> --db <dbname> <dumpfolder>
```

Ou,

```
mongodump --host <hostname> --port <port> --collection <collectionname> <dumpfolder>
```

11. Execute o comando **mongorestore** para restaurar o arquivo dump em qualquer instância do MongoDB. Escolha a instância original do MongoDB para a qual o backup foi criado ou qualquer instância alternativa.

Use o comando apropriado. O primeiro comando é para um banco de dados e o segundo comando é para uma coleção:

```
mongorestore --host <hostname> --port <port> --db <dbname> <dumpfolder>\<dbname>
```

Ou,

```
mongorestore --host <hostname> --port <port> --collection <collectionname> <dumpfolder>\<dbname>
```

12. Quando a operação de restauração de banco de dados ou de coleta for concluída, acesse **Tarefas e operações > Recursos ativos**.
13. Clique em **Ações > Cancelar restauração** para terminar o procedimento de restauração granular.

Fazendo backup e restaurando dados do SQL Server

Para proteger o conteúdo em um SQL Server, primeiro registre a instância do SQL Server para que ela seja reconhecida pelo IBM Spectrum Protect Plus. Em seguida, crie tarefas para operações de backup e restauração.

Requisitos de Sistema

Certifique-se de que seu ambiente SQL Server atenda aos requisitos do sistema em [“Microsoft Requisitos do SQL Server”](#) na página 41.

Registro e autenticação

Registre cada servidor SQL Server no IBM Spectrum Protect Plus por nome ou endereço IP. Ao registrar um nó do Cluster SQL Server (AlwaysOn), registre cada nó por nome ou endereço IP. Observe que os endereços IP devem ser voltados ao público e devem atender na porta 5985. O nome completo do domínio e o nome de DNS do nó da máquina virtual devem ser resolvíveis e roteáveis a partir do dispositivo IBM Spectrum Protect Plus.

A identidade do usuário deve ter direitos suficientes para instalar e iniciar o Serviço de Ferramentas do IBM Spectrum Protect Plus no nó, incluindo o direito **Efetuar logon como um serviço**. Para obter informações adicionais sobre este direito, consulte [Incluir o direito Efetuar logon como um serviço em uma conta](#).

A política de segurança padrão usa o protocolo Windows NTLM, e o formato de identidade do usuário segue o formato padrão *domain\name*.

Quando estiver usando objetos de política de grupo (GPO) do Windows, a configuração do objeto de política de grupo, o nível de autenticação de **Network security: LAN Manager** deve ser configurado corretamente. Configure-o com uma das seguintes opções:

- Não Definido
- Enviar apenas resposta NTLMv2
- Envie apenas a resposta NTLMv2. Refuse LM
- Envie apenas a resposta NTLMv2. Refuse LM & NTLM

Requisitos do Kerberos

A autenticação baseada no Kerberos pode ser ativada por meio de um arquivo de configuração no dispositivo IBM Spectrum Protect Plus. Isso substituirá o protocolo Windows NTLM padrão.

Somente para autenticação baseada no Kerberos, a identidade do usuário deve ser especificada no formato *username@FQDN*. O nome do usuário deve ser capaz de autenticar-se usando a senha registrada para obter um chamado de concessão de chamado (TGT) do centro de distribuição de chaves (KDC) no domínio especificado pelo nome completo do domínio.

A autenticação do Kerberos também requer que o clock skew entre o Controlador de domínio e o dispositivo IBM Spectrum Protect Plus seja menor que cinco minutos.

O protocolo Windows NTLM padrão não é dependente de tempo.

Privilégios

No servidor SQL Server, a credencial de login do sistema deve ter permissões públicas e sysadmin ativadas, além da permissão para acessar recursos de cluster em um ambiente SQL Server AlwaysOn. Se uma conta do usuário for usada para todas as funções do SQL Server, um login do Windows deverá ser ativado para o servidor SQL Server, com permissões públicas e sysadmin ativadas.

Cada instância do SQL Server pode usar uma conta do usuário específica para acessar os recursos dessa instância específica.

Para concluir operações de backup do log, o usuário do SQL Server registrado no IBM Spectrum Protect Plus deve ter a permissão sysadmin ativada para gerenciar tarefas do agente do SQL Server.

O Planejador de Tarefas do Windows é usado para planejar backups do log. Dependendo do ambiente, os usuários podem receber o erro a seguir: *Uma sessão de logon especificada não existe. Ela pode já ter sido finalizada.* Isso ocorre devido a uma configuração de Política de grupo de acesso à rede que precisa ser desativada. Para obter mais informações sobre como desativar esse GPO, consulte o artigo de Suporte da Microsoft a seguir: <https://support.microsoft.com/en-us/help/968264/error-message-when-you-try-to-map-to-a-network-drive-of-a-dfs-share-by>

Incluindo um servidor de aplicativos SQL Server

Quando um servidor de aplicativos SQL Server for incluído, um inventário das instâncias e dos bancos de dados que estão associados ao servidor de aplicativos será capturado e incluído no IBM Spectrum Protect Plus. Este processo permite concluir tarefas de backup e restauração, bem como executar relatórios.

Procedimento

Para incluir um host do SQL Server, conclua as seguintes etapas.

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > SQL > Backup**.
2. Clique em **Gerenciar servidores de aplicativos**.
3. Clique em **Incluir Servidor de Aplicativos**.
4. Preencha os campos na área de janela **Propriedades do aplicativo**:

Endereço do Host

Insira o endereço IP resolvível ou um caminho e nome de máquina resolvíveis.

Utilizar usuário existente

Ative para selecionar um nome do usuário e senha inseridos anteriormente para o provedor.

UserID

Insira seu nome de usuário para o provedor. A identidade do usuário segue o formato padrão *domain \name* se a máquina virtual for conectada a um domínio. O formato *local _administrator* será usado se o usuário for um administrador local.

Somente para autenticação baseada no Kerberos, a identidade do usuário deve ser especificada no formato *username@FQDN*. O nome do usuário deve ser capaz de autenticar-se usando a senha registrada para obter um chamado de concessão de chamado (TGT) do centro de distribuição de chaves (KDC) no domínio especificado pelo nome completo do domínio.

Senha

Insira sua senha para o provedor.

Máximo de bancos de dados simultâneos

Configure o número máximo de bancos de dados para backup simultâneo no servidor. O desempenho do servidor é afetado durante o backup simultâneo de um grande número de bancos de dados, já que cada banco de dados utiliza vários encadeamentos e consome largura da banda ao copiar dados. Use esta opção para controlar o impacto nos recursos do servidor e minimizar o impacto em operações de produção.

5. Clique em **Salvar**. O IBM Spectrum Protect Plus confirma uma conexão de rede, inclui o servidor de aplicativos no banco de dados do IBM Spectrum Protect Plus e, em seguida, cataloga a instância.

Se aparecer uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se suas entradas estiverem corretas e a conexão for malsucedida, entre em contato com um administrador do sistema para revisar as conexões.

O que Fazer Depois

Depois de incluir o servidor de aplicativos SQL Server, conclua a seguinte ação:

Ação	Como
Designar permissões de usuário ao servidor de aplicativos.	Consulte “Criando uma função” na página 302 .

Conceitos relacionados

[“Gerenciando o acesso de” na página 297](#)

Usando o controle de acesso baseado na função, é possível configurar os recursos e permissões disponíveis para contas do usuário do IBM Spectrum Protect Plus.

Tarefas relacionadas

[“Fazendo Backup dos Dados do SQL Server” na página 225](#)

Use uma tarefa de backup para fazer backup de ambientes SQL Server com capturas instantâneas.

[“Restaurando os Dados do SQL Server” na página 228](#)

Use uma tarefa de restauração para restaurar um ambiente do Microsoft SQL Server a partir de capturas instantâneas. Depois de executar as tarefas de Restauração Instantânea de Disco do IBM Spectrum Protect Plus, seus clones do SQL Server poderão ser usados imediatamente. IBM Spectrum Protect Plus cataloga e rastreia todas as instâncias clonadas.

Detectando recursos do SQL Server

Os recursos do SQL Server são detectados automaticamente depois que o servidor de aplicativos é incluído no IBM Spectrum Protect Plus. No entanto, é possível executar uma tarefa de inventário para detectar quaisquer mudanças que ocorreram desde a inclusão do servidor de aplicativos.

Procedimento

Para executar uma tarefa de inventário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > SQL > Backup**.
2. Na lista de instâncias do SQL Server, selecione uma instância ou clique no link para a instância para navegar para o recurso desejado. Por exemplo, se desejar executar uma tarefa de inventário para um banco de dados individual na instância, clique no link da instância e, em seguida, selecione uma máquina virtual.
3. Clique em **Executar Inventário**.

Testando a conexão com um servidor de aplicativos SQL Server

É possível testar a conexão com um host do SQL Server. A função de teste verifica a comunicação com o host e testa as configurações de DNS entre o dispositivo virtual IBM Spectrum Protect e o host.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > SQL > Backup**.
2. Clique em **Gerenciar servidores de aplicativos**.
3. Na lista de hosts, clique em **Testar** no menu **Ações** para o host.

Fazendo Backup dos Dados do SQL Server

Use uma tarefa de backup para fazer backup de ambientes SQL Server com capturas instantâneas.

Antes de Iniciar

Durante o backup de base inicial, o IBM Spectrum Protect Plus cria um novo volume vSnap e cria um compartilhamento NFS. Durante backups incrementais, o volume criado anteriormente é reutilizado. O agente do IBM Spectrum Protect Plus monta o compartilhamento no servidor SQL Server no qual o backup deve ser concluído.

Quando o backup estiver concluído, o agente do IBM Spectrum Protect Plus desmontará o compartilhamento do servidor SQL Server e criará uma captura instantânea do vSnap do volume de backup.

Revise as informações a seguir:

- Antes de um usuário do IBM Spectrum Protect Plus poder implementar operações de backup e restauração, as funções e grupos de recursos devem ser designados ao usuário. Conceda aos usuários acesso a recursos e a operações de backup e restauração por meio da área de janela **Contas**. Para obter mais informações, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#).
- O Inicializador iSCSI da Microsoft deve estar ativado e em execução no servidor Windows. Deve ser ativada uma rota iSCSI entre o sistema SQL e o servidor vSnap. Para obter mais informações, consulte [Microsoft iSCSI Initiator Step-by-Step Guide](#).
- Evite configurar o backup do log para um único banco de dados SQL por meio de várias tarefas de backup. Os logs são truncados durante as operações de backup do log. Se um único banco de dados SQL for incluído em várias definições de tarefa com o backup do log ativado, um backup do log de uma tarefa irá truncar um log antes de ele ser submetido a backup pela próxima tarefa. Isso pode causar falha das tarefas de restauração point-in-time.
- O IBM Spectrum Protect Plus não suporta o backup do log de modelos de recuperação simples.
- Antes de copiar logs para vSnap, o SPP usa a pasta de backup configurada para a instância do SQL Server como a área de migração de dados para coletar logs. O volume no qual essa pasta está localizada deve ter espaço suficiente disponível para conter todos os logs de transações entre as tarefas de backup. A área de preparação de dados pode ser modificada alterando a configuração da pasta de backup, usando o SQL Server Management Studio (SSMS).
- O failover de uma instância de cluster SQL durante o backup não é suportado.

- Se você planeja fazer backup de um grande número de bancos de dados, poderá ser necessário aumentar o número do máximo de encadeamentos do trabalhador em cada instância do SQL Server associada para assegurar que as tarefas de backup sejam concluídas com sucesso. O valor padrão para o máximo de encadeamentos do trabalhador é 0. O servidor determina automaticamente o valor máximo de encadeamentos do trabalhador com base no número de processadores disponíveis para o servidor. O SQL Server usa os encadeamentos deste conjunto para conexões de rede, pontos de verificação de banco de dados e consultas. Além disso, um backup de cada banco de dados requer um encadeamento adicional a partir desse conjunto. Se você tiver um grande número de bancos de dados em uma tarefa de backup, o máximo padrão de encadeamentos do trabalhador poderá não ser suficiente para fazer backup de todos os bancos de dados e a tarefa falhará. Para obter informações adicionais sobre como aumentar a opção do máximo de encadeamentos do trabalhador, consulte [Configurar a opção de configuração do servidor máximo de encadeamentos do trabalhador](#).
- Quando um backup do log de um banco de dados secundário SQL Always On falha com o seguinte erro, a preferência de backup do grupo de disponibilidade deve ser mudada para Primária:

```
O backup do log para o banco de dados 'DatabaseName' em uma réplica secundária falhou porque um ponto de sincronização não pôde ser estabelecido no banco de dados principal.
```

Mudar a preferência para Primária irá fazer backup do log a partir da réplica principal. Após a conclusão de um backup do log bem-sucedido da réplica principal, a preferência de backup poderá ser mudada.

Execute as seguintes ações:

- Registre os provedores dos quais você deseja fazer backup. Para obter mais informações, consulte [“Incluindo um servidor de aplicativos SQL Server”](#) na página 223.
- Configure políticas do SLA. Para obter mais informações, consulte [“Criar políticas de backup”](#) na página 73.
- Antes de configurar e executar tarefas de backup SQL, deve-se definir as configurações de armazenamento de Cópia de sombra para os volumes em que seus bancos de dados SQL estão localizados. Esta configuração é definida uma vez por volume. Se novos bancos de dados forem incluídos na tarefa, a configuração deverá ser definida para todos os novos volumes contendo bancos de dados SQL. No Windows Explorer, clique com o botão direito no volume de origem e selecione a guia **Cópias de sombra**. Configure o **Tamanho máximo** para **Sem limite** ou um tamanho razoável, dependendo do tamanho do volume de origem e das atividades de E/S, em seguida, clique em **OK**. A área de armazenamento de cópia de sombra deve estar no mesmo volume ou em outro volume disponível durante o tempo de backup.

Procedimento

Para definir uma tarefa de backup SQL, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > SQL**.
2. Selecione uma instância do SQL Server para fazer backup.

Use a função de procura para procurar instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**. As opções disponíveis são **Cluster Independente/de Failover** e **Sempre ativo**.
3. Clique em **Selecionar uma política SLA** para incluir uma ou mais políticas SLA que atendam aos seus critérios de dados de backup para a definição de tarefa.
4. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.

A tarefa é executada conforme definido pelas políticas de SLA selecionadas. Para executar a tarefa manualmente, clique em **Tarefas e operações > Planejamento**. Selecione a tarefa e clique em **Ações > Iniciar**.

Dica: o botão **Executar** é ativado somente para um único backup de banco de dados e o banco de dados deve ter uma política de ANS aplicada.
5. Para editar opções antes de criar a definição de tarefa, clique em **Selecionar opções**. Configure as opções de definição de tarefa.

Ativar Backup de Log

Selecione para permitir que o IBM Spectrum Protect Plus faça backup de logs de transações e, em seguida, proteja os discos subjacentes.

O IBM Spectrum Protect Plus trunca automaticamente os backups do log posteriores de bancos de dados dos quais ele faz backup. Se os logs do banco de dados não forem submetidos a backup com o IBM Spectrum Protect Plus, os logs não serão truncados pelo IBM Spectrum Protect Plus e devem ser gerenciados separadamente.

Quando uma tarefa de backup SQL for concluída com backups do log ativados, todos os logs de transações até o ponto de conclusão da tarefa serão limpos do servidor SQL Server. A limpeza de log ocorrerá somente se a tarefa de backup SQL for concluída com sucesso. Se os backups do log forem desativados durante uma nova execução da tarefa, a limpeza do log não ocorrerá.

Se um banco de dados de origem for sobrescrito, todos os logs de transações antigos até esse ponto serão colocados em um diretório “condensado” após a conclusão da restauração do banco de dados original. Quando a próxima execução da tarefa de Backup SQL for concluída, o conteúdo da pasta condensada será removido.

Para concluir backups do log, o usuário do serviço do agente SQL Server deve ser um administrador local do Windows e deve ter a permissão sysadmin ativada para gerenciar as tarefas do agente SQL Server. O agente usará essa conta do administrador para ativar e acessar as tarefas de backup do log. O usuário do serviço do agente SQL Server do IBM Spectrum Protect Plus também deve ser igual ao serviço SQL Server e à conta do serviço do agente SQL Server para cada instância do SQL Server a ser protegida.

Os arquivos de log SQL são armazenados temporariamente em uma área de preparação local antes de serem copiados para um compartilhamento de CIFS. O destino do backup padrão do SQL server serve como a área de preparação e deve ter espaço livre suficiente para armazenar temporariamente os arquivos de log de transações antes de serem copiados para o compartilhamento de CIFS.

Para ativar a criação do planejamento de backup do log para vários bancos de dados na mesma instância do SQL Server, certifique-se de que todos os bancos de dados sejam incluídos na mesma política de ANS.

Quando esta opção é selecionada, as opções de restauração point-in-time estão disponíveis para operações de restauração SQL.

Máximo de Fluxos Paralelo por Banco de Dados

Configure o máximo de fluxos de dados por banco de dados para o armazenamento de backup. Esta configuração se aplica a cada banco de dados na definição de tarefa. Vários bancos de dados podem ser submetidos a backup em paralelo, se o valor da opção estiver configurado como **1**. Vários fluxos paralelos podem melhorar a velocidade de backup, mas o alto consumo de largura da banda pode afetar o desempenho geral do sistema.

6. Quando estiver satisfeito com as informações corretas específicas da tarefa, clique em **Salvar**.

A tarefa é executada conforme definido por sua política de ANS ou pode ser executada manualmente a partir da área de janela Monitor de tarefas.

7. Para configurar opções adicionais, clique no campo **Opções de política** que está associado à tarefa na seção **Status de política de ANS**. Configure as opções de política adicionais:

Pré-scripts e post-scripts

Execute um pré-script ou um post-script. Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de uma tarefa. Os scripts Batch e PowerShell são suportados.

Na seção **Pré-script** ou **Pós-script**, selecione um script transferido por upload e um servidor de aplicativos ou de script no qual o script será executado. Para selecionar um servidor de aplicativos no qual o script será executado, desmarque a caixa de seleção **Usar servidor de script**. Os scripts e servidores de script são configurados na página **Configuração do sistema > Script**.

Para continuar executando a tarefa se o script associado à tarefa falhar, selecione **Continuar a tarefa durante erro do script**.

Quando esta opção é ativada, se um pré-script ou pós-script concluir o processamento com um código de retorno diferente de zero, será feita uma tentativa de operação de backup ou de restauração e o status da tarefa de pré-script será relatado como CONCLUÍDO. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa de pós-script será relatado como CONCLUÍDO.

Quando esta opção é desativada, não é feita tentativa de backup ou de restauração e o status da tarefa de pré-script ou pós-script é relatado como COM FALHA.

Recursos de Exclusão

Exclua recursos específicos da tarefa de backup por meio de um único padrão ou de vários padrões de exclusão. Os recursos podem ser excluídos por meio de uma correspondência exata ou com asteriscos curinga especificados antes do padrão (*test) ou depois do padrão (test*).

Vários curingas asteriscos também são suportados em um único padrão. Os padrões suportam caracteres alfanuméricos padrão, bem como os seguintes caracteres especiais: - _ e *.

Separe vários filtros com um ponto-e-vírgula.

Forçar Backup Completo de Recursos

Force operações de backup de base para máquinas virtuais específicas ou bancos de dados na definição de tarefa de backup. Separe vários recursos com um ponto-e-vírgula.

8. Para salvar as opções adicionais configuradas, clique em **Salvar**.

O que Fazer Depois

Depois de criar a definição de tarefa de backup, conclua a seguinte ação:

Ação	Como
Crie uma definição de tarefa de Restauração SQL.	Consulte “Restaurando os Dados do SQL Server” na página 228.

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração”](#) na página 255

Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de tarefas de backup e restauração no nível de tarefa. Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts são criados localmente, transferidos por upload para seu ambiente por meio da página **Script** e, em seguida, aplicados a definições de tarefa.

Tarefas relacionadas

[“Iniciando Tarefas”](#) na página 252

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Restaurando os Dados do SQL Server

Use uma tarefa de restauração para restaurar um ambiente do Microsoft SQL Server a partir de capturas instantâneas. Depois de executar as tarefas de Restauração Instantânea de Disco do IBM Spectrum Protect Plus, seus clones do SQL Server poderão ser usados imediatamente. IBM Spectrum Protect Plus cataloga e rastreia todas as instâncias clonadas.

Antes de Iniciar

Conclua os pré-requisitos a seguir:

- Crie e execute uma tarefa de backup de SQL. Para obter instruções, consulte [“Fazendo Backup dos Dados do SQL Server”](#) na página 225.
- Para que um usuário do IBM Spectrum Protect Plus possa restaurar dados, as funções e os grupos de recursos apropriados devem ser designados ao usuário. Conceda aos usuários acesso aos recursos e às

operações de backup e restauração usando a área de janela **Contas**. Para obter instruções, consulte [Capítulo 13, “Gerenciando o acesso de”, na página 297](#).

- Se você estiver planejando executar uma recuperação de momento, certifique-se de que o serviço de instância SQL de destino de restauração e o serviço IBM Spectrum Protect Plus SQL Server usem a mesma conta do usuário.

Revise as restrições e considerações a seguir:

- Se você estiver planejando executar uma operação de restauração de produção para um cluster failover do SQL Server, o volume-raiz do caminho de arquivo alternativo deverá ser elegível para o banco de dados do host e para os arquivos de log. O volume deve pertencer ao grupo de recursos do servidor de cluster do SQL Server de destino e ser uma dependência do servidor de cluster do SQL Server.
- Não é possível restaurar dados para um volume compactado NTFS ou FAT devido às restrições do banco de dados SQL Server. Para obter mais informações, consulte [Descrição de suporte para bancos de dados SQL Server em volumes compactados](#).
- Se você estiver planejando restaurar dados para um local alternativo, o destino do SQL Server deverá estar executando a mesma versão do SQL Server ou uma versão mais recente. Para obter mais informações, consulte [Suporte de Compatibilidade](#).
- Quando você estiver restaurando dados para uma instância primária em um ambiente do grupo de disponibilidade do SQL Always On, o banco de dados será incluído no grupo de banco de dados de destino Always On. Após a operação de restauração primária, o SQL server define um valor inicial para o banco de dados secundário em ambientes em que a definição automática de valor inicial é suportada (Microsoft SQL Server 2016 e mais recente). Em seguida, o banco de dados é ativado no grupo de disponibilidade de destino. O tempo de sincronização depende da quantidade de dados que está sendo transferida e da conexão entre as réplicas principais e secundárias.

Se a definição automática de valor inicial não for suportada ou não estiver ativada, uma restauração secundária a partir do ponto de restauração com o intervalo de Número de Sequência de Log (LSN) mais curto da instância primária deverá ser concluída. Os backups de log com o ponto de restauração point-in-time mais recente criados pelo IBM Spectrum Protect Plus devem ser restaurados caso o backup do log tenha sido ativado na instância primária. A operação de restauração do banco de dados secundário é concluída no estado RESTORING e o comando **T-SQL** deve ser emitido para incluir o banco de dados no grupo de destinos. Para obter mais informações, consulte [Transact-Referência de SQL \(Mecanismo de Banco de Dados\)](#).

- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Sobre Esta Tarefa

A Restauração de disco instantânea usa o protocolo iSCSI para montar imediatamente os LUNs sem transferir dados. Os bancos de dados para os quais as capturas instantâneas foram obtidas são catalogados e podem ser recuperados instantaneamente sem transferência física de dados.

Os seguintes modos de restauração são suportados:

Modo de acesso instantâneo

No modo de acesso instantâneo, nenhuma ação adicional será executada após a montagem do compartilhamento. Os usuários podem concluir qualquer recuperação customizada usando os arquivos no volume vSnap. Uma restauração de acesso instantâneo de um banco de dados Always On é realizada para a instância de destino local.

Modo de teste

No modo de teste, o agente cria um novo banco de dados usando os arquivos de dados diretamente a partir do volume vSnap.

Modo de produção

No modo de produção, o agente primeiro restaura os arquivos do volume vSnap de volta para o armazenamento primário e, em seguida, cria o novo banco de dados usando os arquivos restaurados.

Procedimento

Para definir uma tarefa de restauração SQL, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > SQL > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > SQL**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, execute as ações a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. É possível alternar as origens exibidas para mostrar as instâncias do SQL Server em um ambiente independente ou em cluster ou grupos de disponibilidade Always On usando o filtro **Visualizar**.

Também é possível usar a função de procura para procurar bancos de dados nas instâncias ou nos grupos de disponibilidade.
 - b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados. Para remover um item da origem da lista, clique no ícone de menos  ao lado do item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar. Alguns campos não são exibidos até que um campo relacionado seja selecionado.

Opção	Descrição
Tipo de Restauração	Selecione o tipo de tarefa de restauração: On-demand: captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. On-demand: momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.
Tipo de local da restauração	Selecione um tipo de local a partir do qual os dados serão restaurados: Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site . Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem .

Opção	Descrição
	<p>Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	<p>Se estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
Seletor de Data	<p>Para operações de restauração on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo de datas.</p>
Ponto de Restauração	<p>Para operações de restauração on demand, selecione uma captura instantânea a partir da lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, especifique onde você deseja restaurar o banco de dados e clique em **Avançar.**

Restaurar para a instância original

Selecione essa opção para restaurar o banco de dados para a instância original.

Restaurar para a instância primária

Para operações de restauração em um ambiente SQL Always On, selecione esta opção para restaurar o banco de dados para a instância primária do grupo de disponibilidade do Always On. O banco de dados é incluído de volta no grupo.

Restaurar para instância alternativa

Selecione esta opção para restaurar o banco de dados para um destino local que seja diferente da instância original e, em seguida, selecione o local alternativo na lista de servidores disponíveis.

Para operações de restauração em um ambiente SQL Always On no modo de teste, o banco de dados de disponibilidade de origem é restaurado para a instância de destino selecionada.

Para operações de restauração em um ambiente SQL Always On no modo de produção, o banco de dados restaurado será incluído no grupo de disponibilidade de destino se a instância de destino for uma réplica principal. Se a instância de destino for uma réplica secundária do grupo de disponibilidade de destino, o banco de dados será restaurado para a réplica secundária e deixado no estado de restauração.

Se a opção de definição automática de valores iniciais estiver ativada para o grupo de disponibilidade de destino, os caminhos do banco de dados secundário serão sincronizados com o banco de dados principal. Se o log do banco de dados primário não estiver truncado, o banco de dados secundário poderá ser incluído no grupo de disponibilidade pelo SQL.

5. Na página **Método de restauração**, configure a tarefa de restauração a ser executada no modo de teste, de produção ou de acesso instantâneo, por padrão.

Para o modo de teste ou de produção, é possível, opcionalmente, inserir um novo nome para o banco de dados restaurado.

Para o modo de produção, também é possível especificar uma nova pasta para o banco de dados restaurado expandindo o banco de dados e inserindo um novo nome de pasta.

Clique em **Avançar** para continuar.

Depois que a tarefa é criada, é possível executá-la no modo de teste, de produção ou de acesso instantâneo na área de janela **Sessões da tarefa**.

6. Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Opções de Recuperação

Configure as opções de recuperação point-in-time a seguir:

Sem recuperação

Configure o banco de dados selecionado para um estado RESTORING. Se você estiver gerenciando backups do log de transações sem usar o IBM Spectrum Protect Plus, será possível restaurar manualmente os arquivos de log e incluir o banco de dados em um grupo de disponibilidade, supondo que o LSN das cópias do banco de dados secundário e primário atenda aos critérios.

Restrição: A opção **Sem recuperação** não suporta operações de restauração de modo de produção para os grupos SQL Always On.

Recuperar até o término do backup

Restaure o banco de dados selecionado para o estado no momento em que o backup foi criado.

Recuperar até um ponto específico no tempo

Quando o backup de log for ativado usando uma definição de tarefa de backup SQL, as opções de restauração de momento estarão disponíveis ao criar uma definição de tarefa de restauração SQL. Selecione uma das seguintes opções:

- **Por Tempo** . Selecione esta opção para configurar uma recuperação de momento a partir de uma data e hora específica.
- **Por ID de transação** . Selecione esta opção para configurar uma recuperação point-in-time por ID de transação.

Em uma operação de restauração independente, o IBM Spectrum Protect Plus localiza os pontos de restauração que continuam e seguem diretamente o momento selecionado. Durante a recuperação, são montados o volume de backup de dados mais antigo e o volume de backup de log mais recente. Se o momento for após a última operação de backup, um ponto de restauração temporário será criado.

Ao executar operações de restauração em um ambiente SQL Always On no modo de teste, o banco de dados restaurado se associará à instância na qual o grupo de disponibilidade reside.

Ao executar operações de restauração em um ambiente SQL Always On no modo de produção, o banco de dados principal restaurado é associado ao grupo de disponibilidade. Se a opção de definição automática de valores iniciais estiver ativada para o grupo de disponibilidade de destino, os caminhos do banco de dados secundário serão sincronizados com o banco de dados principal. Se o log do banco de dados primário não estiver truncado, o banco de dados secundário poderá ser incluído no grupo de disponibilidade pelo SQL.

Opções do Aplicativo

Configure as opções do aplicativo:

Sobrescrever banco de dados existente

Ative a tarefa de restauração para sobrescrever o banco de dados selecionado. Por padrão, esta opção não é ativada.

Dica: Antes de executar as operações de restauração em um ambiente SQL Always On usando o modo de produção com a opção **Sobrescrever banco de dados existente**, assegure-se de que o banco de dados não esteja presente nas réplicas do grupo de disponibilidade de destino. Para isso, deve-se limpar manualmente os bancos de dados originais (para serem sobrescritos) de todas as réplicas do grupo de disponibilidade de destino.

Máximo de Fluxos Paralelo por Banco de Dados

Configure o número máximo de fluxos de dados paralelos a partir do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Se o valor da opção estiver configurado como 1, vários bancos de dados ainda poderão ser restaurados em paralelo. Múltiplos fluxos paralelos podem melhorar a velocidade da restauração, porém o consumo alto de largura da banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas ao restaurar um banco de dados do SQL Server para seu local original usando seu nome do banco de dados original.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Limpe automaticamente os recursos alocados como parte de uma operação de restauração, se a recuperação falhar.

Permitir sobrescrição de sessão

Selecione esta opção para substituir um banco de dados existente por um banco de dados com o mesmo nome durante a recuperação. Quando uma Restauração de disco instantânea for executada para um banco de dados e outro banco de dados com o mesmo nome já estiver em execução no host ou cluster de destino, o IBM Spectrum Protect Plus encerrará o banco de dados existente antes de iniciar o banco de dados recuperado. Se essa opção não for selecionada, a tarefa de restauração falhará quando o IBM Spectrum Protect Plus detectar um banco de dados em execução com o mesmo nome.

Continuar com restaurações de outros bancos de dados mesmo que um falhe

Altere a recuperação de um recurso em uma série se a recuperação do recurso anterior falhar. Se essa opção não for ativada, a tarefa de restauração será interrompida se a recuperação de um recurso falhar.

Prioridade de protocolo (somente Acesso Instantâneo)

Se mais de um protocolo de armazenamento estiver disponível, selecione o protocolo para ter prioridade na tarefa. Os protocolos disponíveis são **iSCSI** e **Fibre Channel**.

Prefixo do Ponto de Montagem

Para operações de restauração de acesso instantâneo, especifique o prefixo para o caminho para onde o ponto de montagem será direcionado.

7. Opcional: Na página **Aplicar scripts**, especifique os scripts que podem ser executados antes ou depois de uma operação ser executada no nível da tarefa. Os scripts Batch e PowerShell são suportados.

Pré-Script

Marque essa caixa de seleção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pré-script será executado. Para selecionar um servidor de aplicativos no qual o pré-script será executado, desmarque a caixa de seleção **Usar servidor de script**. Scripts e servidores de script são configurados na página **Configuração do sistema > Script**.

Pós-script

Selecione essa opção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pós-script será executado. Para selecionar um servidor de aplicativos no qual o pós-script será executado, desmarque a caixa de seleção **Usar servidor de script**. Scripts e servidores de script são configurados na página **Configuração do sistema > Script**.

Continuar job/tarefa no erro de script

Marque essa caixa de seleção para continuar executando a tarefa, se o script que estiver associado à tarefa falhar.

Ao marcar essa caixa de seleção, se um pré-script ou pós-script concluir o processamento com um código de retorno diferente de zero, a operação de backup ou de restauração será tentada e o status da tarefa de pré-script será relatado como COMPLETED. Se um pós-script concluir o processamento com um código de retorno diferente de zero, o status da tarefa de pós-script será relatado como COMPLETED.

Se você desmarcar essa caixa de seleção, a operação de backup ou de restauração não será tentada e o status da tarefa de pré-script ou pós-script será relatado como FAILED.

8. Execute uma das ações a seguir na página **Planejamento**:
 - Se estiver executando uma tarefa on demand, clique em **Avançar**.
 - Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

Resultados

Uma tarefa on demand é iniciada após você clicar em **Enviar** e o registro **onDemandRestore** é incluído na área de janela **Sessões da tarefa** brevemente. Para visualizar o progresso da operação de restauração, expanda a tarefa. Também será possível fazer download do arquivo de log clicando no ícone de download



Uma tarefa recorrente será iniciada no horário de início planejado quando você iniciar o planejamento na página **Tarefas e operações > Schedule**.

Todas as tarefas em execução são visualizáveis na página **Tarefas e operações > Tarefas em execução**.

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração”](#) na página 255

Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de tarefas de backup e restauração no nível de tarefa. Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts são criados localmente, transferidos por upload para seu ambiente por meio da página **Script** e, em seguida, aplicados a definições de tarefa.

Tarefas relacionadas

[“Incluindo um servidor de aplicativos SQL Server”](#) na página 223

Quando um servidor de aplicativos SQL Server for incluído, um inventário das instâncias e dos bancos de dados que estão associados ao servidor de aplicativos será capturado e incluído no IBM Spectrum Protect Plus. Este processo permite concluir tarefas de backup e restauração, bem como executar relatórios.

“Fazendo Backup dos Dados do SQL Server” na página 225

Use uma tarefa de backup para fazer backup de ambientes SQL Server com capturas instantâneas.

Fazendo Backup e Restaurando Dados do Oracle

Para proteger o conteúdo do Oracle, primeiro registre a instância do Oracle para que ela seja reconhecida pelo IBM Spectrum Protect Plus. Em seguida, crie tarefas para operações de backup e restauração.

Certifique-se de que seu ambiente Oracle atenda aos requisitos do sistema em “Requisitos do Oracle” na página 37.

Incluindo um servidor de aplicativos Oracle

Quando um servidor de aplicativos Oracle é incluído, um inventário das instâncias e bancos de dados que estão associados ao servidor de aplicativos é capturado e incluído no IBM Spectrum Protect Plus. Este processo permite concluir tarefas de backup e restauração, bem como executar relatórios.

Procedimento

Para registrar um servidor de aplicativos Oracle, conclua as seguintes etapas.

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Oracle > Backup**.
2. Clique em **Gerenciar servidores de aplicativos**.
3. Clique em **Incluir servidor de aplicativos** para incluir a máquina host.
4. Na área de janela **Propriedades do aplicativo**, insira o endereço do host.
O endereço do host é um endereço IP resolvível ou um caminho e nome de máquina resolvíveis.
5. Selecione **Usuário** ou **Chave SSH**.

Opção	Descrição
Usuário	<p>Clique nesta opção para especificar um usuário existente ou insira um ID do usuário e senha. O usuário deve ter privilégios sudo configurados. Preencha os campos conforme a seguir:</p> <p>Utilizar usuário existente Selecione esta caixa de seleção para usar um nome de usuário e senha inseridos anteriormente para o servidor de aplicativos. Selecione um nome de usuário da lista Selecionar usuário.</p> <p>UserID Insira seu nome de usuário para o servidor de aplicativos. Se a máquina virtual estiver conectada a um domínio, a identidade do usuário seguirá o formato padrão <i>domain\name</i>. Se o usuário for um administrador local, use o formato <i>local_administrator</i>.</p> <p>Somente para autenticação baseada no Kerberos, a identidade do usuário deve ser especificada no formato <i>username@FQDN</i>. O nome do usuário deve ser capaz de autenticar-se usando a senha registrada para obter um chamado de concessão de chamado (TGT) do centro de distribuição de chaves (KDC) no domínio especificado pelo nome completo do domínio.</p> <p>Password Insira sua senha para o servidor de aplicativos.</p>
Chave SSH	<p>Clique nesta opção para usar uma chave SSH. Selecione uma chave da lista Selecionar uma chave SSH.</p>

6. Para proteger bancos de dados multiencadeados no Oracle 12c e versões mais recentes, forneça credenciais para os bancos de dados:
 - a) Clique em **Obter bancos de dados** para detectar e listar os bancos de dados Oracle no servidor host que está sendo incluído.
Cada banco de dados Oracle é listado com seu nome, status e uma indicação se as credenciais foram especificadas anteriormente para o banco de dados.
 - b) Para cada banco de dados multiencadeado que você deseja proteger, clique em **Configurar credencial** e especifique o ID do usuário e a senha. Como alternativa, é possível selecionar um usuário existente da lista **Selecionar usuário**.
Deve-se especificar as credenciais para um usuário do banco de dados Oracle que tenha privilégios SYSDBA.
7. Em **Máximo de bancos de dados simultâneos**, configure o número máximo de bancos de dados para backup simultâneo no servidor.
O desempenho do servidor é afetado quando muitos bancos de dados são submetidos a backup simultaneamente, pois cada banco de dados utiliza vários encadeamentos e consome largura de banda quando copia dados. Use esta opção para controlar o impacto nos recursos do servidor e minimizar o impacto em operações de produção.
8. Clique em **Salvar**. O IBM Spectrum Protect Plus confirma uma conexão de rede, inclui o servidor de aplicativos no banco de dados do IBM Spectrum Protect Plus e, em seguida, cataloga a instância.
Se aparecer uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se suas entradas estiverem corretas e a conexão for malsucedida, entre em contato com um administrador do sistema para revisar as conexões.

O que Fazer Depois

Depois de incluir o servidor de aplicativos Oracle, conclua a seguinte ação:

Ação	Como
Designar permissões de usuário ao servidor de aplicativos.	Consulte “Criando uma função” na página 302 .

Conceitos relacionados

[“Gerenciando o acesso de” na página 297](#)

Usando o controle de acesso baseado na função, é possível configurar os recursos e permissões disponíveis para contas do usuário do IBM Spectrum Protect Plus.

Tarefas relacionadas

[“Fazendo Backup de Dados do Oracle” na página 237](#)

Use uma tarefa de backup para fazer backup de ambientes Oracle com capturas instantâneas.

[“Restaurando dados do Oracle” na página 240](#)

Use uma tarefa de restauração para restaurar um ambiente do Oracle a partir de capturas instantâneas. O IBM Spectrum Protect Plus cria um clone do vSnap a partir da versão que é selecionada durante a criação da definição de tarefa e cria um compartilhamento do Network File System (NFS). Em seguida, o agente do IBM Spectrum Protect Plus monta o compartilhamento no servidor Oracle no qual a tarefa de restauração deve ser executada. Para o Oracle Real Application Clusters (RAC), a tarefa de restauração é executada em todos os nós no cluster.

Detectando recursos do Oracle

Os recursos do Oracle são detectados automaticamente depois que o servidor de aplicativos é incluído no IBM Spectrum Protect Plus. No entanto, é possível executar uma tarefa de inventário para detectar quaisquer mudanças que ocorreram desde a inclusão do servidor de aplicativos.

Procedimento

Para executar uma tarefa de inventário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Oracle > Backup**.

2. Na lista de instâncias do Oracle, selecione uma instância ou clique no link para a instância para navegar para o recurso desejado. Por exemplo, se desejar executar uma tarefa de inventário para um banco de dados individual na instância, clique no link da instância e, em seguida, selecione uma máquina virtual.
3. Clique em **Executar Inventário**.

Testando a conexão com um servidor de aplicativos Oracle

É possível testar a conexão com um host Oracle. A função de teste verifica a comunicação com o host e testa as configurações de DNS entre o dispositivo virtual IBM Spectrum Protect e o host.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Oracle > Backup**.
2. Clique em **Gerenciar servidores de aplicativos**.
3. Na lista de hosts, clique em **Testar** no menu **Ações** para o host.

Fazendo Backup de Dados do Oracle

Use uma tarefa de backup para fazer backup de ambientes Oracle com capturas instantâneas.

Antes de Iniciar

Revise as informações a seguir:

- Para assegurar que as permissões do sistema de arquivos sejam retidas corretamente quando o IBM Spectrum Protect Plus mover dados do Oracle entre servidores, certifique-se de que os IDs do usuário e do grupo dos usuários do Oracle (por exemplo, oracle, oinstall, dba) sejam consistentes em todos os servidores. Consulte a documentação do Oracle para obter os valores de uid e gid recomendados.
- Se uma tarefa de inventário do Oracle for executada ao mesmo tempo ou em um curto período após uma tarefa de backup do Oracle, podem ocorrer erros de cópia devido a montagens temporárias que são criadas durante a tarefa de backup. Como uma melhor prática, planeje tarefas de inventário do Oracle para que elas não se sobreponham com tarefas de backup do Oracle.
- Evite configurar o backup do log para um único banco de dados Oracle usando várias tarefas de backup. Se um único banco de dados Oracle for incluído em várias definições de tarefa com o backup do log ativado, um backup do log de uma tarefa poderá truncar um log antes de ele ser submetido a backup pela próxima tarefa. Isso pode causar falha das tarefas de restauração point-in-time.
- A recuperação point-in-time não é suportada quando um ou mais arquivos de dados são incluídos no banco de dados no período entre o point-in-time escolhido e o horário em que a tarefa de backup anterior foi executada.

Execute as seguintes ações:

- Antes de um usuário do IBM Spectrum Protect Plus poder implementar operações de backup e restauração, as funções e grupos de recursos devem ser designados ao usuário. Conceda aos usuários acesso a recursos e a operações de backup e restauração por meio da área de janela **Contas**. Para obter mais informações, consulte [Capítulo 13, “Gerenciando o acesso de”](#), na página 297.
- Registre os provedores dos quais você deseja fazer backup. Para obter mais informações, consulte [“Incluindo um servidor de aplicativos Oracle”](#) na página 235.
- Configure políticas do SLA. Para obter mais informações, consulte [“Criar políticas de backup”](#) na página 73.

Sobre Esta Tarefa

Usando o backup de base inicial, o IBM Spectrum Protect Plus cria um volume vSnap e um compartilhamento NFS. Durante backups incrementais, o volume criado anteriormente é reutilizado. O agente do IBM Spectrum Protect Plus monta o compartilhamento no servidor Oracle no qual o backup deve ser concluído.

No caso do Oracle Real Application Clusters (RAC), o backup é concluído a partir de qualquer nó no cluster. Quando o backup estiver concluído, o agente do IBM Spectrum Protect Plus desmontará o compartilhamento do servidor Oracle e criará uma captura instantânea vSnap do volume de backup.

O IBM Spectrum Protect Plus pode proteger bancos de dados multiencadeados no Oracle 12c e versões mais recentes. Para obter instruções sobre como ativar o IBM Spectrum Protect Plus para proteger bancos de dados multiencadeados, consulte [“Incluindo um servidor de aplicativos Oracle”](#) na página 235.

Procedimento

Para definir uma tarefa de backup do Oracle, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Oracle**.
2. Selecione diretórios iniciais, bancos de dados Oracle e grupos de discos do ASM para backup. Use a função de procura para procurar instâncias disponíveis.
3. Clique em **Selecionar uma política SLA** para incluir uma ou mais políticas SLA que atendam aos seus critérios de dados de backup para a definição de tarefa.

4. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.

A tarefa é executada conforme definido pelas políticas de SLA selecionadas. Para executar a tarefa manualmente, clique em **Tarefas e operações > Planejamento**. Selecione a tarefa e clique em **Ações > Iniciar**.

Dica: o botão **Executar** é ativado somente para um único backup de banco de dados e o banco de dados deve ter uma política de ANS aplicada.

5. Para editar opções antes de criar a definição de tarefa, clique em **Selecionar opções**. Configure as opções de definição de tarefa.

Ativar Backup de Log

A opção **Ativar backup do log** deve ser selecionada para permitir restauração point-in-time do Oracle.

Selecione **Ativar backup do log** para permitir que o IBM Spectrum Protect Plus crie automaticamente um volume de backup do log e monte-o no servidor de aplicativos. Portanto, o IBM Spectrum Protect Plus descobre automaticamente o local do log primário arquivado existente e usa cron para configurar uma tarefa planejada. A tarefa planejada conclui um backup do log de transações do local primário para esse volume de backup do log na frequência especificada por meio da configuração **Frequência**.

A **Frequência** pode ser configurada como um valor independente da frequência de backup de banco de dados especificada nas configurações de Política de ANS. Por exemplo, a Política de ANS pode ser configurada para fazer backup do banco de dados uma vez por dia, enquanto a frequência de backup do log pode ser configurada para uma vez por 30 minutos.

Para o Oracle RAC, o IBM Spectrum Protect Plus monta o volume e configura a tarefa cron em cada um dos nós do cluster. Quando o planejamento é acionado, as tarefas são coordenadas internamente para assegurar que qualquer nó ativo conclua o backup do log e os outros nós não executem nenhuma ação.

O IBM Spectrum Protect Plus gerencia automaticamente a retenção de logs em seu próprio volume de backup do log com base nas configurações de retenção na política de ANS.

Selecione **Truncar logs de origem após o backup bem-sucedido** para excluir automaticamente os logs arquivados mais antigos do local de log arquivado primário do banco de dados. Se a opção for desmarcada, os logs arquivados no destino de log primário não serão excluídos e o Administradores de banco de dados devem continuar gerenciando esses logs usando suas políticas de retenção de log existentes. Se a opção estiver selecionada, o IBM Spectrum Protect Plus excluirá os logs arquivados mais antigos desnecessários do local do log primário no final de cada backup de banco de dados bem-sucedido.

Quando a opção **Truncar logs de origem após o backup bem-sucedido** estiver selecionada, configure a retenção de logs primários por meio da configuração **Retenção de log primário em dias**. Essa configuração controla a quantidade de logs arquivados que são retidos nos locais de logs arquivados primários. Por exemplo, se a opção **Retenção de log primário em dias** estiver configurada como **3**, o

IBM Spectrum Protect Plus excluirá todos os logs arquivados mais antigos que três dias do local do log arquivado primário no final de cada backup de banco de dados bem-sucedido.

Máximo de Fluxos Paralelo por Banco de Dados

Configure o máximo de fluxos de dados por banco de dados para o armazenamento de backup. Esta configuração se aplica a cada banco de dados na definição de tarefa. Vários bancos de dados podem ser submetidos a backup em paralelo, se o valor da opção estiver configurado como **1**. Vários fluxos paralelos podem melhorar a velocidade de backup, mas o alto consumo de largura da banda pode afetar o desempenho geral do sistema.

- Quando estiver satisfeito com as informações corretas específicas da tarefa, clique em **Salvar**.
- Para configurar opções adicionais, clique no campo **Opções de política** que está associado à tarefa na seção **Status de política de ANS**. Configure as opções de política adicionais:

Pré-scripts e Pós-scripts

Execute um pré-script ou um post-script. Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de uma tarefa no nível de tarefa. As máquinas baseadas no Windows suportam scripts de Lote e PowerShell enquanto as máquinas baseadas no Linux suportam shell scripts.

Na seção **Pré-script** ou **Pós-script**, selecione um script transferido por upload e um servidor de aplicativos ou de script no qual o script será executado. Para selecionar um servidor de aplicativos no qual o script será executado, desmarque a caixa de seleção **Usar servidor de script**. Os scripts e servidores de script são configurados por meio da página **Configuração do sistema > Script**.

Para continuar executando a tarefa se o script associado à tarefa falhar, selecione **Continuar a tarefa durante erro do script**.

Quando esta opção é ativada, se um pré-script ou pós-script concluir o processamento com um código de retorno diferente de zero, será feita uma tentativa de operação de backup ou de restauração e o status da tarefa de pré-script será relatado como CONCLUÍDO. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa de pós-script será relatado como CONCLUÍDO.

Quando esta opção é desativada, não é feita tentativa de backup ou de restauração e o status da tarefa de pré-script ou pós-script é relatado como COM FALHA.

Recursos de Exclusão

Exclua recursos específicos da tarefa de backup por meio de um único padrão ou de vários padrões de exclusão. Os recursos podem ser excluídos por meio de uma correspondência exata ou com asteriscos curinga especificados antes do padrão (*test) ou depois do padrão (test*).

Vários curingas asteriscos também são suportados em um único padrão. Os padrões suportam caracteres alfanuméricos padrão, bem como os seguintes caracteres especiais: - _ e *.

Separe vários filtros com um ponto-e-vírgula.

Forçar Backup Completo de Recursos

Forçar operações de backup de base para máquinas virtuais ou bancos de dados específicos na definição da tarefa de backup. Separe vários recursos com um ponto-e-vírgula.

O que Fazer Depois

Depois de criar a definição de tarefa de backup, conclua a seguinte ação:

Ação	Como
Crie uma definição de tarefa do Oracle Restore.	Consulte “Restaurando dados do Oracle” na página 240 .

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração” na página 255](#)

Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de tarefas de backup e restauração no nível de tarefa. Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts são criados localmente, transferidos por upload para seu ambiente por meio da página **Script** e, em seguida, aplicados a definições de tarefa.

Restaurando dados do Oracle

Use uma tarefa de restauração para restaurar um ambiente do Oracle a partir de capturas instantâneas. O IBM Spectrum Protect Plus cria um clone do vSnap a partir da versão que é selecionada durante a criação da definição de tarefa e cria um compartilhamento do Network File System (NFS). Em seguida, o agente do IBM Spectrum Protect Plus monta o compartilhamento no servidor Oracle no qual a tarefa de restauração deve ser executada. Para o Oracle Real Application Clusters (RAC), a tarefa de restauração é executada em todos os nós no cluster.

Antes de Iniciar

Conclua os pré-requisitos a seguir:

- Crie e execute uma tarefa de backup do Oracle. Para obter instruções, consulte [“Fazendo Backup de Dados do Oracle”](#) na página 237.
- Para que um usuário do IBM Spectrum Protect Plus possa restaurar dados, as funções e os grupos de recursos apropriados devem ser designados ao usuário. Conceda aos usuários acesso aos recursos e às operações de backup e restauração usando a área de janela **Contas**. Para obter instruções, consulte [Capítulo 13, “Gerenciando o acesso de”,](#) na página 297.

Revise as seguintes restrições:

- A recuperação de momento não é suportada quando um ou mais arquivos de dados são incluídos no banco de dados no período entre o momento escolhido e o horário em que a tarefa de backup anterior é executada.
- Se um banco de dados Oracle for montado, mas não for aberto durante uma tarefa de backup, o IBM Spectrum Protect Plus não poderá determinar as configurações do banco de dados **tempfile** que estão relacionadas a **autoextensibility** e ao tamanho máximo. Quando um banco de dados é restaurado a partir desse ponto de restauração, o IBM Spectrum Protect Plus não pode recriar o **tempfiles** com as configurações originais porque elas são desconhecidas. Em vez disso, **tempfiles** são criados com configurações padrão, "AUTOEXTEND ON" e "MAXSIZE 32767M". Após a conclusão da tarefa de restauração, é possível atualizar manualmente as configurações.
- Ao restaurar de um archive do IBM Spectrum Protect, os arquivos serão migrados para um conjunto temporário da fita anterior para o início da tarefa. Dependendo do tamanho da restauração, esse processo pode levar várias horas.

Sobre Esta Tarefa

Os seguintes modos de restauração são suportados:

Modo de acesso instantâneo

No modo de acesso instantâneo, nenhuma ação adicional será executada após a montagem do compartilhamento. Os usuários podem concluir qualquer recuperação customizada usando os arquivos no volume vSnap.

Modo de teste

No modo de teste, o agente cria um novo banco de dados usando os arquivos de dados diretamente a partir do volume vSnap.

Modo de produção

No modo de produção, o agente primeiro restaura os arquivos do volume vSnap de volta para o armazenamento primário e, em seguida, cria o novo banco de dados usando os arquivos restaurados.

Procedimento

Para definir uma tarefa de restauração do Oracle, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Aplicativos > Oracle > Criar tarefa de restauração** para abrir o assistente "Restauração de Captura Instantânea".

Dicas:

- Também é possível abrir o assistente "Restauração de captura instantânea" clicando em **Tarefas e operações > Criar operação de restauração > Oracle**.
 - Para obter um resumo em execução de suas seleções no assistente "Restauração de Captura Instantânea", mova o cursor para o ícone de informações  na área de janela de navegação no assistente.
 - Para efetuar bypass das páginas opcionais no assistente, selecione **Ignorar etapas opcionais**.
2. Na página **Seleção de origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para mostrar os bancos de dados que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis e alternar as instâncias exibidas por meio do filtro **Visualizar**.
 - b) Clique no ícone de mais  próximo ao banco de dados que você deseja usar como a origem da operação de restauração. É possível selecionar mais de um banco de dados a partir da lista.

As origens selecionadas são incluídas na lista de restauração ao lado da lista de bancos de dados. Para remover um item da lista, clique no ícone de menos  próximo ao item.
 - c) Clique em **Avançar** para continuar.
 3. Na página **Captura instantânea de origem**, especifique a instância do banco de dados que você deseja restaurar. Preencha os campos a seguir e clique em **Avançar** para continuar. Alguns campos não são exibidos até que um campo relacionado seja selecionado.

Opção	Descrição
Tipo de Restauração	Selecione o tipo de tarefa de restauração: On-demand: captura instantânea Executa uma tarefa de restauração descartável por meio de uma captura instantânea do banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. On-demand: momento Executa uma tarefa de restauração descartável de um backup de momento de um banco de dados. A tarefa de restauração é iniciada imediatamente após a conclusão do assistente. Recorrente Cria uma tarefa de restauração momentânea repetitiva que é executada sob um planejamento.
Tipo de local da restauração	Selecione um tipo de local a partir do qual os dados serão restaurados: Site O site no qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site . Transferência de nuvem O servidor em nuvem para o qual as capturas instantâneas foram transferidas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem . Transferência de repositório O servidor de repositório para o qual as capturas instantâneas foram transferidas. O servidor do repositório é definido na área de janela

Opção	Descrição
	<p>Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de nuvem O servidor em nuvem no qual as capturas instantâneas foram arquivadas. O servidor em nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Nuvem.</p> <p>Archive de repositório O servidor de repositório no qual as capturas instantâneas foram arquivadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
<p>Selecione um local</p>	<p>Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:</p> <p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O local do site primário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Secundário O local do site secundário a partir do qual as capturas instantâneas serão restauradas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>
<p>Seletor de Data</p>	<p>Para operações de restauração de captura instantânea, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro do intervalo de data.</p>
<p>Ponto de Restauração</p>	<p>Para operações de restauração de captura instantânea, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de dados selecionado.</p>
<p>Usar servidor vSnap alternativo para a tarefa de restauração</p>	<p>Se você estiver restaurando dados de um recurso em nuvem ou um servidor do repositório, marque esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Ao restaurar dados de um ponto de restauração que foi transferido ou arquivado para um recurso em nuvem ou um servidor do repositório, um servidor vSnap será usado como um gateway para concluir a operação. Por padrão, o servidor vSnap que é usado para concluir a operação de restauração é o mesmo servidor vSnap que é usado para concluir as operações de backup e de transferência. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

4. Na página **Configurar destino**, especifique onde você deseja restaurar o banco de dados e clique em **Avançar**.

Restaurar para o local original

Selecione essa opção para restaurar o banco de dados para o servidor original.

Restaurar o local alternativo

Selecione esta opção para restaurar o banco de dados para um destino local que seja diferente do servidor original e, em seguida, selecione o local alternativo na lista de servidores disponíveis.

5. Na página **Método de restauração**, configure a tarefa de restauração a ser executada no modo de teste, de produção ou de acesso instantâneo, por padrão.

Para o modo de teste ou de produção, é possível, opcionalmente, inserir um novo nome para o banco de dados restaurado.

Para o modo de produção, também é possível especificar uma nova pasta para o banco de dados restaurado expandindo o banco de dados e inserindo um novo nome de pasta.

Clique em **Avançar** para continuar.

Depois que a tarefa é criada, ela pode ser executada no modo de teste, de produção ou de acesso instantâneo na área de janela **Sessões da tarefa**.

6. Na página **Opções da tarefa**, configure opções adicionais para a tarefa de restauração e clique em **Avançar** para continuar.

Opções de Recuperação

Configure as opções de recuperação point-in-time a seguir:

Recuperar até o término do backup

Restaure o banco de dados selecionado para o estado no momento em que o backup foi criado.

Recuperar até um ponto específico no tempo

Quando o backup de log for ativado usando uma definição de tarefa de Backup do Oracle, as opções de restauração de momento estarão disponíveis ao criar uma definição de tarefa de Restauração do Oracle. Selecione uma das seguintes opções e, em seguida, clique em **Salvar**:

- **Por Tempo** . Selecione esta opção para configurar uma recuperação de momento a partir de uma data e hora específica.
- **Por SCN** . Selecione esta opção para configurar uma recuperação point-in-time pelo System Change Number (SCN).

O IBM Spectrum Protect Plus localiza os pontos de restauração que continuam e seguem diretamente o momento selecionado. Durante a recuperação, são montados o volume de backup de dados mais antigo e o volume de backup de log mais recente. Se o momento tiver ocorrido após o último backup, um ponto de restauração temporário será criado.

Opções do Aplicativo

Configure as opções do aplicativo:

Sobrescrever banco de dados existente

Ative esta opção para permitir que a tarefa de restauração sobrescreva o banco de dados selecionado. Por padrão, essa opção não é selecionada.

Máximo de Fluxos Paralelo por Banco de Dados

Configure o número máximo de fluxos de dados paralelos a partir do armazenamento de backup por banco de dados. Esta configuração se aplica a cada banco de dados na definição de tarefa. Se o valor da opção estiver configurado como 1, vários bancos de dados ainda poderão ser restaurados em paralelo. Múltiplos fluxos paralelos podem melhorar a velocidade da restauração, porém o consumo alto de largura da banda pode afetar o desempenho geral do sistema.

Esta opção é aplicável apenas ao restaurar um banco de dados do Oracle para seu local original usando seu nome de banco de dados original.

Parâmetros de Init

Essa opção controla os parâmetros de inicialização que são usados para iniciar o banco de dados recuperado nos fluxos de trabalho de teste e de produção do Oracle.

Origem. Essa opção é padrão. O IBM Spectrum Protect Plus usa os mesmos parâmetros de inicialização que o banco de dados de origem, mas com as seguintes mudanças:

- Os parâmetros que contêm caminhos como **control_files**, **db_recovery_file_dest** ou **log_archive_dest_*** são atualizados para refletir os novos caminhos com base nos pontos de montagem renomeados dos volumes recuperados.

- Parâmetros, como **audit_file_dest** e **diagnostic_dest**, são atualizados para apontarem para o local apropriado no diretório base do Oracle no servidor de destino, caso o caminho seja diferente do servidor de origem.
- Se um novo nome for especificado para o banco de dados, os parâmetros **db_name** e **db_unique_name** serão atualizados para refletir o novo nome.
- Parâmetros relacionados ao cluster, como **instance_number**, **thread** e **cluster_database** são configurados automaticamente pelo IBM Spectrum Protect Plus, dependendo dos valores adequados para o destino.

Destino . Customize os parâmetros de inicialização especificando um arquivo de modelo que contém os parâmetros de inicialização que são usados pelo IBM Spectrum Protect Plus.

O caminho especificado deve apontar para um arquivo de texto simples que exista no servidor de destino e que seja legível pelo usuário do IBM Spectrum Protect Plus. O arquivo deve estar no formato `pfile` do Oracle, consistindo em linhas no formato a seguir:

```
nome = valor
```

Comentários que começam com o caractere `#` são ignorados.

O IBM Spectrum Protect Plus lê o modelo `pfile` e copia as entradas para o novo `pfile` que é usado para iniciar o banco de dados recuperado. No entanto, os seguintes parâmetros no modelo são ignorados. Em vez disso, o IBM Spectrum Protect Plus configura seus valores para refletir os valores apropriados do banco de dados de origem ou para refletir novos caminhos com base nos pontos de montagem renomeados dos volumes recuperados.

- **control_files**
- **db_block_size**
- **db_create_file_dest**
- **db_recovery_file_dest**
- **log_archive_dest**
- **spfile**
- **undo_tablespace**

Além disso, os parâmetros relacionados ao cluster como **instance_number**, **thread** e **cluster_database** são configurados automaticamente pelo IBM Spectrum Protect Plus, dependendo dos valores adequados para o destino.

Opções Avançadas

Configure as opções avançadas de definição de tarefa:

Executar limpeza imediatamente na falha da tarefa

Ative esta opção para limpar automaticamente os recursos alocados como parte de uma operação de restauração, se a recuperação falhar.

Permitir sobrescrição de sessão

Selecione esta opção para substituir um banco de dados existente por um banco de dados com o mesmo nome durante a recuperação. Quando uma Restauração de disco instantânea for executada para um banco de dados e outro banco de dados com o mesmo nome já estiver em execução no host ou cluster de destino, o IBM Spectrum Protect Plus encerrará o banco de dados existente antes de iniciar o banco de dados recuperado. Se essa opção não for selecionada, a tarefa de restauração falhará quando o IBM Spectrum Protect Plus detectar um banco de dados em execução com o mesmo nome.

Continuar com restaurações de outros bancos de dados mesmo que um falhe

Altere a recuperação de um recurso em uma série se a recuperação do recurso anterior falhar. Se essa opção não for ativada, a tarefa de restauração será interrompida se a recuperação de um recurso falhar.

Prioridade de protocolo (somente Acesso Instantâneo)

Se mais de um protocolo de armazenamento estiver disponível, selecione o protocolo para ter prioridade na tarefa. Os protocolos disponíveis são **iSCSI** e **Fibre Channel**.

Prefixo do Ponto de Montagem

Para operações de restauração de acesso instantâneo, especifique o prefixo para o caminho para onde o ponto de montagem será direcionado.

7. Opcional: Na página **Aplicar scripts**, especifique os scripts que podem ser executados antes ou depois de uma operação ser executada no nível da tarefa. Os scripts Batch e PowerShell são suportados em sistemas operacionais Windows e os scripts de shell são suportados em sistemas operacionais Linux.

Pré-Script

Marque essa caixa de seleção para escolher um script transferido por upload e um servidor de aplicativos ou de script no qual o pré-script será executado. Para selecionar um servidor de aplicativos no qual o pré-script será executado, desmarque a caixa de seleção **Usar servidor de script**. Scripts e servidores de script são configurados na página **Configuração do sistema > Script**.

Pós-script

Marque essa caixa de seleção para escolher um script transferido por upload e um servidor de aplicativos ou de script em que o post-script será executado. Para selecionar um servidor de aplicativos no qual o pós-script será executado, desmarque a caixa de seleção **Usar servidor de script**. Scripts e servidores de script são configurados na página **Configuração do sistema > Script**.

Continuar job/tarefa no erro de script

Marque essa caixa de seleção para continuar executando a tarefa, se o script que estiver associado à tarefa falhar.

Ao marcar essa caixa de seleção, se um pré-script ou pós-script concluir o processamento com um código de retorno diferente de zero, a operação de backup ou de restauração será tentada e o status da tarefa de pré-script será relatado como COMPLETED. Se um pós-script concluir o processamento com um código de retorno diferente de zero, o status da tarefa de pós-script será relatado como COMPLETED.

Se você desmarcar essa caixa de seleção, o backup ou a restauração não será tentada e o status da tarefa de pré-script ou de pós-script será relatado como FAILED.

8. Execute uma das ações a seguir na página **Planejamento**:

- Se estiver executando uma tarefa on demand, clique em **Avançar**.
- Se estiver configurando uma tarefa recorrente, insira um nome para o planejamento de tarefa e especifique a frequência e quando iniciar a tarefa de restauração. Clique em **Avançar**.

9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

Resultados

Uma tarefa on demand é iniciada após você clicar em **Enviar** e o registro **onDemandRestore** é incluído na área de janela **Sessões da tarefa** brevemente. Para visualizar o progresso da operação de restauração, expanda a tarefa. Também será possível fazer download do arquivo de log clicando no ícone de download



Uma tarefa recorrente será iniciada no horário de início planejado quando você iniciar o planejamento na página **Tarefas e operações > Schedule**.

Todas as tarefas em execução são visualizáveis na página **Tarefas e operações > Tarefas em execução**.

O que Fazer Depois

Os bancos de dados Oracle são sempre restaurados no modo não multiencadeado. Se os bancos de dados que foram restaurados estavam originalmente no modo multiencadeado, após a conclusão da

operação de restauração, deve-se configurar manualmente as credenciais e alternar os bancos de dados para o modo multiencadeado.

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração”](#) na página 255

Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de tarefas de backup e restauração no nível de tarefa. Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts são criados localmente, transferidos por upload para seu ambiente por meio da página **Script** e, em seguida, aplicados a definições de tarefa.

Tarefas relacionadas

[“Incluindo um servidor de aplicativos Oracle”](#) na página 235

Quando um servidor de aplicativos Oracle é incluído, um inventário das instâncias e bancos de dados que estão associados ao servidor de aplicativos é capturado e incluído no IBM Spectrum Protect Plus. Este processo permite concluir tarefas de backup e restauração, bem como executar relatórios.

Capítulo 9. Protegendo IBM Spectrum Protect Plus

Proteja o aplicativo IBM Spectrum Protect Plus fazendo backup dos bancos de dados subjacentes para cenários de recuperação de desastre. Definições de configuração, recursos registrados, pontos de restauração, configurações de armazenamento de backup, dados de procura e informações de tarefa são submetidos a backup para um servidor vSnap definido na política de ANS associada.

Fazendo backup do aplicativo IBM Spectrum Protect Plus

Faça backup de definições de configuração, políticas de ANS, recursos registrados, configurações de armazenamento de backup, pontos de restauração, dados de procura e chaves e certificados importados do IBM Spectrum Protect Plus para um servidor vSnap que está definido na política de ANS associada.

Antes de Iniciar

Certifique-se de que a política de ANS apropriada esteja disponível. Para otimizar tarefas de backup, crie políticas de ANS especificamente para fazer backup do IBM Spectrum Protect Plus. Para reduzir o carregamento do sistema, certifique-se de que outras tarefas não estejam planejadas para serem executadas durante a tarefa de backup do IBM Spectrum Protect Plus. Para criar uma política de SLA, consulte [“Criando uma política de SLA”](#) na página 89.

Restrição: Não é possível selecionar o servidor vSnap integrado como o destino da política de ANS de backup do IBM Spectrum Protect Plus. O servidor vSnap integrado é chamado de localhost e é instalado automaticamente quando o dispositivo IBM Spectrum Protect Plus é implementado inicialmente. Selecione um servidor vSnap externo secundário como o destino ao criar uma política de ANS para backup

Um catálogo do IBM Spectrum Protect Plus pode ser restaurado para o mesmo local ou para um local alternativo do IBM Spectrum Protect Plus em cenários de recuperação de desastre.

Procedimento

Para fazer backup de dados do IBM Spectrum Protect Plus :

1. Na área de janela de navegação, clique em **Gerenciar proteção > IBM Spectrum Protect Plus > Backup**.
2. Selecione uma política de ANS para associar à operação de backup do catálogo do IBM Spectrum Protect Plus. A política de ANS define o planejamento do backup do catálogo, junto com as configurações de destino, de replicação e de transferência do backup. Os dados de backup de catálogo também podem ser transferidos para recursos em nuvem e servidores de repositório.
3. Clique em **Salvar** para criar a definição de tarefa.

Resultados

A tarefa é executada conforme definido pelas políticas de SLA selecionadas ou pode ser executada manualmente, clicando em **Tarefas e operações > Planejamento**. Em seguida, selecione a tarefa na guia **Planejamento** e clique em **Ações > Iniciar**. Para obter instruções, consulte [“Inicie a tarefa de backup”](#) na página 79.

Restaurando o aplicativo IBM Spectrum Protect Plus

Restaurar as definições de configuração, pontos de restauração, dados de procura e informações de tarefas do IBM Spectrum Protect Plus que foram submetidos a backup para o servidor vSnap. Os dados podem ser restaurados para o mesmo local ou outro local do IBM Spectrum Protect Plus.

Sobre Esta Tarefa



Atenção: Uma operação de restauração do IBM Spectrum Protect Plus sobrescreve todos os dados no dispositivo virtual IBM Spectrum Protect Plus ou local alternativo do dispositivo virtual. Todas as operações do IBM Spectrum Protect Plus param enquanto os dados estão sendo restaurados. A interface com o usuário não está acessível e todas as tarefas que estão em execução serão canceladas. Todas as capturas instantâneas criadas entre as operações de backup e restauração não serão salvas.

Se estiver restaurando um backup em nuvem transferido, o recurso em nuvem ou o servidor do repositório deverá ser registrado no local alternativo do IBM Spectrum Protect Plus.

Procedimento

Para restaurar dados do IBM Spectrum Protect Plus :

1. Na área de janela de navegação, clique em **Gerenciar proteção > IBM Spectrum Protect Plus > Restauração**.
2. Selecione um servidor vSnap, um recurso em nuvem ou servidor do repositório.

Os dados podem ser restaurados no mesmo local ou em um local alternativo em cenários de recuperação de desastre.

As capturas instantâneas disponíveis para o servidor são exibidas.
3. Clique em **Restaurar** para a captura instantânea do catálogo que você deseja restaurar.
4. Selecione um dos seguintes modos de restauração:

Restaurar o catálogo e suspender todas as tarefas planejadas

O catálogo é restaurado e todas as tarefas planejadas são deixadas em um estado suspenso. Nenhuma tarefa planejada é iniciada, o que permite a validação e o teste de entradas no catálogo e a criação de novas tarefas. Geralmente, essa opção é usada em casos de uso do DevOps.

Restaurar o catálogo

O catálogo é restaurado e todas as tarefas planejadas continuam a ser executadas como capturadas no backup do catálogo. Geralmente, essa opção é usada na recuperação de desastre.

5. Clique em **Restaurar**.
6. Para executar a tarefa de restauração, na caixa de diálogo, clique em **Sim**.

Gerenciando IBM Spectrum Protect Plus pontos de restauração

É possível usar a área de janela **Retenção de ponto de restauração** para procurar pontos de restauração no catálogo do IBM Spectrum Protect Plus por nome da tarefa de backup, visualizar suas datas de criação e expiração e substituir a retenção designada.

Sobre Esta Tarefa

A expiração de uma sessão de tarefa não removerá uma captura instantânea e o ponto de recuperação relacionado se a captura instantânea estiver bloqueada por um relacionamento de replicação ou de transferência. Execute a tarefa ativada para replicação ou transferência para mudar o bloqueio para uma captura instantânea mais recente. A captura instantânea e o ponto de recuperação serão removidos durante a próxima execução da tarefa de manutenção.

Procedimento

Para configurar uma sessão de tarefa para expirar:

1. Na área de janela de navegação, clique em **Gerenciar proteção > IBM Spectrum Protect Plus > Retenção de ponto de restauração**.
2. Na guia Sessões de backup, procure a sessão de tarefa ou o ponto de restauração desejado. Para obter informações adicionais sobre como usar a função de procura, consulte [Apêndice A, “Diretrizes de Procura”, na página 315](#).

3. Use filtros para otimizar sua procura em tipos de tarefa e intervalo de data quando a tarefa de backup associada tiver sido iniciada.
4. Clique no ícone procurar .
5. Selecione as sessões de tarefas que você deseja expirar.
6. Na lista **Ações**, selecione uma das seguintes opções:
 - **Expirar** é usado para expirar uma única sessão de tarefa.
 - **Expirar todas as sessões de tarefas** é usado para expirar todas as sessões de tarefas não expiradas para a tarefa selecionada.
7. Para confirmar a expiração, na caixa de diálogo, clique em **Sim**.

Resultados

A sessão de tarefa é removida durante a próxima execução da tarefa de manutenção.

Conceitos relacionados

[“Tipos de Tarefa” na página 251](#)

As tarefas são usadas para executar operações de backup, restauração, manutenção e inventário no IBM Spectrum Protect Plus.

Excluindo IBM Spectrum Protect Plus recursos do catálogo

É possível usar a guia **Máquinas virtuais/Bancos de dados** na área de janela **Retenção do ponto de restauração** para expirar metadados do catálogo que estão associados a um recurso do catálogo do IBM Spectrum Protect Plus. Os recursos são incluídos no catálogo por meio de tarefas de inventário. Expirar um recurso remove os metadados associados a um ponto de restauração do catálogo, que libera espaço no catálogo e remove o ponto de restauração das telas de recuperação.

Sobre Esta Tarefa

Expirar um recurso do catálogo não remove capturas instantâneas associadas de um servidor vSnap ou armazenamento de backup secundário.

Procedimento

Para expirar um recurso do catálogo:

1. Na área de janela de navegação, clique em **Gerenciar proteção > IBM Spectrum Protect Plus > Retenção de ponto de restauração**.
2. Clique na guia **Máquinas Virtuais / Bancos de Dados**.
3. Use o filtro para procurar por tipo de recurso e, em seguida, insira uma sequência de procura para procurar um recurso por nome. Para obter informações adicionais sobre como usar a função de procura, consulte [Apêndice A, “Diretrizes de Procura”, na página 315](#).
4. Clique no ícone procurar .
5. Clique no ícone excluir  que está associado a um recurso.
6. Para confirmar a expiração, na caixa de diálogo, clique em **Sim**.

Resultados

Os metadados do catálogo associados com o recurso são removidos do catálogo.

Conceitos relacionados

[“Tipos de Tarefa” na página 251](#)

As tarefas são usadas para executar operações de backup, restauração, manutenção e inventário no IBM Spectrum Protect Plus.

Capítulo 10. Tarefas e operações

Use a janela **Tarefas e operações** para monitorar tarefas, revisar o histórico da tarefa, planejar tarefas, visualizar recursos ativos e executar novamente ou pausar tarefas e planejamentos.

Para visualizar e gerenciar tarefas e recursos, clique em **Tarefas e operações** e clique na guia apropriada:

- **Tarefas em execução** Mostra as tarefas de backup, inventário, manutenção e restauração que estão em execução.
- **Histórico da tarefa** Mostra as tarefas cujo processamento falhou ou foi concluído com avisos ou as tarefas que foram executadas com sucesso. É possível fazer download de um log da tarefa na página selecionando a tarefa e clicando em **Download.zip**.
- **Recursos ativos** Mostra recursos ativos do aplicativo e do hypervisor.
- **Schedule** Mostra os planejamentos de tarefa. É possível iniciar uma tarefa on demand ou pausar um planejamento de uma tarefa selecionada. Usando o ícone de edição, , também é possível editar um planejamento de tarefa.

Também é possível criar tarefas de restauração on demand ou recorrentes, clicando em **Criar tarefa de restauração**. Para obter instruções sobre como criar tarefas de restauração, clique nos links na tabela a seguir:

Tarefa	Instruções
Criar tarefas de restauração para hypervisors	Consulte os tópicos a seguir: <ul style="list-style-type: none">• “Restaurando Dados do VMware” na página 111• “Restaurando dados do Hyper-V” na página 127
Criar tarefas de restauração para aplicativos	Consulte os tópicos a seguir: <ul style="list-style-type: none">• “Restaurando Dados do Db2 ” na página 151• “Restaurando Microsoft Exchange bancos de dados ” na página 168• “Restaurando Dados do MongoDB ” na página 208• “Restaurando dados do Oracle” na página 240• “Restaurando os Dados do SQL Server” na página 228

Tipos de Tarefa

As tarefas são usadas para executar operações de backup, restauração, manutenção e inventário no IBM Spectrum Protect Plus.

As tarefas de backup e restauração são definidas pelo usuário. Depois de criar essas tarefas, é possível modificá-las a qualquer momento. As tarefas de manutenção e de inventário são predefinidas e não modificáveis.

É possível executar todas as tarefas on demand, mesmo que elas estejam configuradas para execução em um planejamento. Também é possível reter e liberar tarefas que estão configuradas para execução em um planejamento.

Os tipos de tarefas a seguir estão disponíveis:

Backup

Uma tarefa de backup define os recursos dos quais você deseja fazer backup e a política ou políticas de acordo de nível de serviço (ANS) que você deseja aplicar a esses recursos. Cada política de ANS define quando a tarefa é executada. É possível executar a tarefa usando o planejamento definido pela política de ANS ou executar a tarefa on demand.

O nome da tarefa é gerado automaticamente e é construído do tipo de recurso seguido pela política de ANS que é usada para a tarefa. Por exemplo, uma tarefa de backup para os recursos do SQL Server que estão associados à política de ANS Ouro é `sql_Gold`.

Restaurar

Uma tarefa de restauração define o ponto de restauração do qual você deseja restaurar dados. Por exemplo, se estiver restaurando dados do hypervisor, o ponto de restauração pode ser uma máquina virtual. Se estiver restaurando dados do aplicativo, o ponto de restauração pode ser um banco de dados. É possível criar um planejamento para executar a tarefa ou executar a tarefa on demand.

O nome da tarefa depende se você executa a tarefa on demand ou em um planejamento. Se você executar uma operação de restauração on demand, o nome da tarefa `onDemandRestore` será gerado automaticamente.

Se criar uma tarefa para ser executada em um planejamento, você deve especificar um nome de tarefa.

Manutenção

A tarefa de manutenção é executada uma vez por dia para remover recursos e objetos associados que são criados pelo IBM Spectrum Protect Plus quando uma tarefa que está em um estado pendente é excluída.

O procedimento de limpeza recupera o espaço nos dispositivos de armazenamento, limpa o catálogo do IBM Spectrum Protect Plus e remove capturas instantâneas relacionadas. A tarefa de manutenção também remove dados catalogados que estão associados a tarefas excluídas.

O nome da tarefa é `Maintenance`

Inventário

Uma tarefa de inventário é executada automaticamente quando um recurso é incluído no IBM Spectrum Protect Plus. No entanto, é possível executar uma tarefa de inventário a qualquer momento para detectar quaisquer mudanças que ocorreram desde que o recurso foi incluído.

Os nomes de tarefas de inventário são `Default Application Server Inventory`, `Default Hypervisor Inventory` e `Default Storage Server Inventory`.

Iniciando Tarefas

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Procedimento

Conclua as seguintes etapas para iniciar uma tarefa:

1. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.
2. Escolha a tarefa que deseja executar e clique em **Ações > Iniciar**.
A tarefa é iniciada e incluída na guia **Tarefas em execução**.

O que Fazer Depois

Para visualizar o log da tarefa em detalhes, clique na tarefa na guia **Tarefas em execução**.

A tela de log mostra os detalhes a seguir:

- Status: mostra se a mensagem é um erro, um aviso ou uma mensagem informativa.

- Horário: mostra o registro de data e hora da mensagem.
- ID: mostra o identificador exclusivo para a mensagem, se aplicável.
- Descrição: mostra o texto da mensagem.

É possível fazer download de um log da tarefa na página clicando em **Download.zip**. Para cancelar a tarefa, clique em **Ações > Cancelar**.

Pausando e Continuando Tarefas

É possível pausar e continuar uma tarefa planejada ou uma tarefa que está em execução. Quando você pausar uma tarefa planejada, a tarefa não será executada até que seja continuada.

Procedimento

Para pausar e liberar planejamentos de tarefas, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.
2. Escolha a tarefa que deseja pausar e clique em **Ações > Planejamento de pausa**.
3. Para continuar o planejamento de tarefa, clique em **Ações > Liberar planejamento**.

Cancelando Tarefas

É possível cancelar uma tarefa que está em execução.

Procedimento

Para cancelar uma tarefa, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.
2. Para cancelar uma sessão de tarefa em execução, clique no menu **Ações** que está associado à tarefa e, em seguida, clique em **Cancelar**.

Executando novamente as tarefas de backup parcialmente concluídas

Se a última instância de uma tarefa de backup foi parcialmente concluída, será possível executar novamente a tarefa para fazer backup de máquinas virtuais e bancos de dados que foram ignorados.

Sobre Esta Tarefa

Uma tarefa de backup pode ser executada novamente apenas no mesmo ID de sessão que a tarefa de backup original parcialmente concluída. Nenhum backup bem-sucedido do mesmo recurso pode ter sido concluído desde a tarefa de backup parcial que você escolher para executar novamente.

Nota: As tarefas de backup podem ser executadas novamente apenas em resposta a uma falha de backup do hypervisor ou do banco de dados. Os eventos a seguir não se qualificam para operações de nova execução da tarefa de backup:

- Um backup da VM foi concluído com uma falha de FLI.
- Ocorreu uma falha de condensação de captura instantânea para um sistema de armazenamento.
- Uma tarefa de backup falhou com um problema desconhecido, como um erro de catalogação.
- Um recurso está ausente do vCenter.

Para aplicativos para os quais backups de log são suportados, os backups de log não são desativados ao usar o recurso de nova execução. Os backups de log serão desativados para os bancos de dados

aplicáveis na próxima vez em que a tarefa for iniciada, sem usar o recurso de backup on-demand ou de nova execução.

Procedimento

Conclua as seguintes etapas para executar novamente uma operação de backup parcialmente concluída:

1. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Histórico da tarefa**.
2. Use a função de procura e filtros para localizar a última instância da tarefa de backup que foi parcialmente concluída.
3. Selecione a instância da tarefa e, em seguida, clique em **Executar novamente**.

Nota:

Se a tarefa de backup não puder ser executada novamente, a opção **Executar novamente** não estará disponível.

Todas as opções de ANS e quaisquer exclusões que estão associadas à tarefa original são incluídas na operação de nova execução. Nenhuma mudança de opção ou de exclusão é aplicada desde o backup parcialmente concluído. Se a tarefa de nova execução for concluída com sucesso, o resumo da tarefa será atualizado para mostrar sucesso.

Fazendo Backup de um Recurso Único

Se um hypervisor ou servidor de aplicativos estiver associado a uma política de ANS, uma única máquina virtual ou aplicativo poderá ser submetido a backup imediatamente, executando uma operação de backup on-demand. Selecione **Executar** em uma tela de backup do hypervisor ou do servidor de aplicativos para executar uma operação de backup on-demand. Essa opção é ativada quando uma política de ANS existente está associada ao recurso.

Sobre Esta Tarefa

A nova execução de uma tarefa de backup para um único recurso é aplicável apenas para operações de backup, não para operações de replicação ou de transferência.

Para aplicativos para os quais backups de log são suportados, os backups de log não são desativados ao usar o recurso de backup on-demand ou de nova execução. Os backups de log serão desativados para os bancos de dados aplicáveis na próxima vez em que a tarefa for iniciada, sem usar o recurso de backup on-demand ou de nova execução.

Procedimento

Conclua as seguintes etapas para executar uma tarefa de backup on-demand de uma única máquina virtual ou servidor de aplicativos:

1. Na área de janela de navegação, clique em **Gerenciar proteção**. Dependendo do tipo de operação de backup, selecione **Hypervisors > Backup** ou **Aplicativos > Backup**.
2. Clique em uma das instâncias listadas para mostrar a máquina virtual ou recursos do aplicativo associados.

O hypervisor ou o servidor de aplicativos deve estar associado a uma política de ANS existente.

3. Clique em **Executar**.

Se a máquina virtual ou o aplicativo for membro de várias políticas de ANS, selecione a política de ANS a ser executada para a tarefa on-demand.

4. Para confirmar a tarefa de backup, na caixa de diálogo, clique em **OK**.

Configurando scripts para operações de backup e restauração

Pré-scripts e pós-scripts são scripts que podem ser executados antes ou depois da execução de tarefas de backup e restauração no nível de tarefa. Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts são criados localmente, transferidos por upload para seu ambiente por meio da página **Script** e, em seguida, aplicados a definições de tarefa.

Antes de Começar

Revise as seguintes considerações para usar scripts com hypervisors:

- O usuário que está executando o script deve ter o direito **Efetuar logon como um serviço** ativado, que é necessário para executar pré-scripts e pós-scripts. Para obter informações adicionais sobre este direito, consulte [Incluir o direito Efetuar logon como um serviço em uma conta](#).
- O Windows Remote Shell (WinRM) deve estar ativado.

Fazendo Upload de um Script

Os scripts suportados incluem shell scripts para máquinas baseadas no Linux e scripts em Lote e PowerShell para máquinas baseadas no Windows. Os scripts devem ser criados usando o formato de arquivo associado para o sistema operacional.

Procedimento

Conclua as seguintes etapas para fazer upload de um script:

1. Na área de janela de navegação, clique em **Configuração do sistema > Script**.
2. Na seção **Scripts**, clique em **Fazer upload de script**.
A área de janela **Fazer Upload de Script** é exibida.
3. Clique em **Procurar** para selecionar um script local para upload.
4. Clique em **Salvar**.
O script é exibido na tabela **Scripts** e pode ser aplicado a tarefas suportadas.

O que Fazer Depois

Depois de fazer upload do script, conclua a seguinte ação:

Ação	Como
Inclua o script em um servidor a partir do qual ele será executado.	Consulte “Incluindo um script em um servidor” na página 255 .

Incluindo um script em um servidor

Inclua o script em um servidor a partir do qual ele será executado.

Procedimento

Conclua as seguintes etapas para designar um script a um servidor:

1. Na área de janela de navegação, clique em **Configuração do sistema > Script**.
2. Na seção **Servidores de script**, clique em **Incluir servidor de script**.
A área de janela **Propriedades do Servidor de Script** é exibida.
3. Configure as opções do servidor.

Endereço do Host

Insira o endereço IP resolvível ou um caminho e nome de máquina resolvíveis.

Utilizar usuário existente

Ative para selecionar um nome do usuário e senha inseridos anteriormente para o provedor.

Nome de Usuário

Insira seu nome de usuário para o provedor. Se estiver inserindo um SQL server, a identidade do usuário seguirá o formato padrão *domain\name* se a máquina virtual estiver conectada a um domínio. O formato *local_administrator* será usado se o usuário for um administrador local.

Password

Insira sua senha para o provedor.

Tipo de S.O.

Selecione o sistema operacional do servidor de aplicativos.

4. Clique em **Salvar**.

Capítulo 11. Configurando e mantendo o ambiente do sistema IBM Spectrum Protect Plus

As tarefas de gerenciamento de sistemas abrangem a inclusão de armazenamento de backup, o gerenciamento de sites, o registro de servidores Lightweight Directory Access Protocol (LDAP) ou de Protocolo Simples de Transporte de Correio (SMTP) e o gerenciamento de chaves e certificados para recursos em nuvem.

As tarefas de manutenção incluem a revisão da configuração do dispositivo virtual IBM Spectrum Protect Plus, a coleta de arquivos de log para resolução de problemas e o gerenciamento de certificados Secure Sockets Layer (SSL).

Na maioria dos casos, o IBM Spectrum Protect Plus é instalado em um dispositivo virtual. O dispositivo virtual contém o aplicativo e o inventário. As tarefas de manutenção são concluídas no vSphere Client, usando a linha de comandos do IBM Spectrum Protect Plus ou em um console de gerenciamento baseado na web.

As tarefas de manutenção são concluídas por um administrador do sistema. Um administrador do sistema geralmente é um usuário de nível sênior que projetou ou implementou a infraestrutura de vSphere e ESX, ou um usuário com entendimento de uso da linha de comandos do IBM Spectrum Protect Plus, VMware e Linux.

As atualizações de infraestrutura são gerenciadas por recursos de atualização da IBM. O console administrativo serve como o principal meio de atualizar recursos do IBM Spectrum Protect Plus e componentes da infraestrutura subjacentes, incluindo o sistema operacional e o sistema de arquivos. Os pacotes de atualizações do Z File System (ZFS) também são fornecidos para instâncias independentes do vSnap.



Atenção: Atualize os componentes subjacentes do IBM Spectrum Protect Plus usando somente os recursos de atualização fornecidos pela IBM.

Gerenciando o armazenamento de backup secundário

O servidor vSnap é o local de backup primário para capturas instantâneas. Todos os ambientes do IBM Spectrum Protect Plus têm pelo menos um servidor vSnap. Opcionalmente, é possível transferir capturas instantâneas de um servidor vSnap para um sistema de armazenamento em nuvem ou para um servidor do repositório.

Para obter informações sobre como transferir dados de captura instantânea para o armazenamento secundário, consulte [“Transfload para armazenamento de backup secundário”](#) na página 6.

Gerenciando o armazenamento em

É possível transferir para o armazenamento em nuvem para proteção de dados de longo prazo.

Incluindo um armazenamento em nuvem do Amazon S3 como um provedor de armazenamento de backup

Inclua o armazenamento em nuvem do Amazon S3 para permitir que o IBM Spectrum Protect Plus transfira dados para o S3.

Antes de Iniciar

Configure a chave que é necessária para o objeto de nuvem. Para obter instruções, consulte [“Incluindo uma chave de acesso”](#) na página 269.

Certifique-se de que haja depósitos de armazenamento em nuvem criados para os dados do IBM Spectrum Protect Plus antes de incluir o armazenamento em nuvem nas seguintes etapas. Para obter informações sobre como criar depósitos, consulte [Documentação do Amazon Simple Storage Service](#).

Procedimento

Para incluir o armazenamento em nuvem do Amazon S3 como provedor de armazenamento de backup, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Nuvem**.
2. Clique em **Incluir Nuvem**.
3. Na lista **Provedor**, selecione **Amazon S3**.
4. Preencha os campos na área de janela **Registro em nuvem**:

Nome

Insira um nome significativo para ajudar a identificar o armazenamento em nuvem.

Região

Selecione o terminal regional do Amazon Web Services (AWS) do armazenamento em nuvem.

Utilizar a chave existente

Ative para selecionar uma chave inserida anteriormente para o armazenamento e, em seguida, selecione a chave da lista **Selecionar uma chave**.

Se você não selecionar esta opção, preencha os seguintes campos para incluir uma chave:

Nome principal

Insira um nome significativo para ajudar a identificar a chave.

Chave de acesso

Insira a chave de acesso do AWS. As chaves de acesso são criadas por meio do AWS Management Console.

Chave secreta

Insira a chave secreta AWS. Chaves secretas são criadas por meio do AWS Management Console.

5. Clique em **Obter depósitos** e, em seguida, selecione um depósito para servir como o destino de transferência.
Após a geração dos depósitos, os campos **Depósito de transferência** e **Depósito de archive** são exibidos.
6. No campo **Depósito de transferência**, selecione um depósito para servir como o destino de transferência.
7. Opcional: No campo **Depósito de archive**, selecione um recurso de armazenamento em nuvem para servir como o destino de archive.
O arquivamento de dados cria uma cópia completa dos dados e pode fornecer benefícios de longo prazo de proteção, custo e segurança. Para obter mais informações sobre como arquivar dados, consulte as informações sobre como copiar dados para o armazenamento de archive em nuvem no [“Transfload para armazenamento de backup secundário” na página 6](#).
8. Clique em **Registrar**.
O armazenamento em nuvem foi incluído na tabela de servidores em nuvem.

O que Fazer Depois

Depois de incluir o armazenamento do S3, conclua a seguinte ação:

Ação	Como
Associar o armazenamento em nuvem à política de ANS que é usada para a tarefa de backup.	Para criar uma política de SLA, consulte “Criando uma política de SLA” na página 89. Para modificar uma política de ANS existente, consulte “Editando uma política de SLA” na página 93.

Incluindo o IBM Cloud Object Storage como um provedor de armazenamento de backup

Inclua o IBM Cloud Object Storage para permitir que o IBM Spectrum Protect Plus transfira dados para o IBM Cloud.

Antes de Iniciar

Configure a chave e o certificado que são necessários para o objeto de nuvem. Para obter instruções, consulte [“Incluindo uma chave de acesso”](#) na página 269 e [“Incluindo um Certificado”](#) na página 269.

Certifique-se de que haja depósitos de armazenamento em nuvem criados para os dados do IBM Spectrum Protect Plus antes de incluir o armazenamento em nuvem nas seguintes etapas. Para obter informações sobre como criar depósitos, consulte [Sobre o IBM Cloud Object Storage](#).

Procedimento

Para incluir o IBM Cloud Object Storage como um provedor de armazenamento de backup, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Nuvem**.
2. Clique em **Incluir Nuvem**.
3. Na lista **Provedor**, selecione **IBM Cloud Object Storage**.
4. Preencha os campos na área de janela **Registro em nuvem**:

Nome

Insira um nome significativo para ajudar a identificar o armazenamento em nuvem.

Terminal

Selecione o terminal do armazenamento em nuvem.

Utilizar a chave existente

Ative para selecionar uma chave inserida anteriormente para o armazenamento e, em seguida, selecione a chave da lista **Selecionar uma chave**.

Se você não selecionar esta opção, preencha os seguintes campos para incluir uma chave:

Nome principal

Insira um nome significativo para ajudar a identificar a chave.

Chave de acesso

Insira a chave de acesso.

Chave secreta

Insira a chave secreta.

Certificado

Selecione um método de associação de um certificado com o recurso:

Fazer Upload

Selecione e clique em **Procurar** para localizar o certificado e, em seguida, clique em **Fazer upload**.

Copiar e colar

Selecione para inserir o nome do certificado, copiar e colar os conteúdos do certificado, em seguida, clique em **Criar**.

Utilizar existente

Selecione para usar um certificado transferido por upload anteriormente.

Um certificado não será necessário se você estiver incluindo o IBM Cloud Object Storage público.

5. Clique em **Obter depósitos** e, em seguida, selecione um depósito para servir como o destino de transferência.
Após a geração dos depósitos, os campos **Depósito de transferência** e **Depósito de archive** são exibidos.
6. No campo **Depósito de transferência**, selecione um depósito para servir como o destino de transferência.

7. Opcional: No campo **Depósito de archive** , selecione um recurso de armazenamento em nuvem para servir como o destino de archive.

O arquivamento de dados cria uma cópia completa dos dados e pode fornecer os benefícios de longo prazo de proteção, custo e segurança. Para obter mais informações sobre como arquivar dados, consulte as informações sobre como copiar dados para o armazenamento de archive em nuvem no [“Transfload para armazenamento de backup secundário” na página 6.](#)

8. Clique em **Registrar** .

O armazenamento em nuvem foi incluído na tabela de servidores em nuvem.

O que Fazer Depois

Depois de incluir o IBM Cloud Object Storage, conclua a seguinte ação:

Ação	Como
Associar o armazenamento em nuvem à política de ANS que é usada para a tarefa de backup.	Para criar uma política de SLA, consulte “Criando uma política de SLA” na página 89. Para modificar uma política de ANS existente, consulte “Editando uma política de SLA” na página 93.

Incluindo armazenamento em nuvem do Microsoft Azure como um provedor de armazenamento de backup

Inclua o armazenamento em nuvem do Microsoft Azure para permitir que o IBM Spectrum Protect Plus transfira dados para o armazenamento de Blob do Microsoft Azure.

Antes de Iniciar

Certifique-se de que haja depósitos de armazenamento em nuvem criados para os dados do IBM Spectrum Protect Plus antes de incluir o armazenamento em nuvem nas seguintes etapas. Para obter informações sobre como criar depósitos, consulte a documentação do Azure.

Procedimento

Para incluir o armazenamento em nuvem do Microsoft Azure como o provedor de armazenamento de backup, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Armazenamento de backup > Nuvem.**
2. Clique em **Incluir Nuvem** .
3. Na lista **Provedor**, selecione **Armazenamento de blob do Microsoft Azure.**
4. Preencha os campos na área de janela **Registro em nuvem:**

Nome

Insira um nome significativo para ajudar a identificar o armazenamento em nuvem.

Terminal

Selecione o terminal do armazenamento em nuvem.

Utilizar a chave existente

Ative para selecionar uma chave inserida anteriormente para o armazenamento e, em seguida, selecione a chave da lista **Selecionar uma chave.**

Se você não selecionar esta opção, preencha os seguintes campos para incluir uma chave:

Nome principal

Insira um nome significativo para ajudar a identificar a chave.

Nome da conta de armazenamento

Insira o nome da conta de armazenamento de acesso do Microsoft Azure. Isso é a partir do Portal de Gerenciamento do Azure.

Chave Compartilhada da Conta de Armazenamento

Insira a chave do Microsoft Azure a partir de qualquer um dos campos-chave no Portal de Gerenciamento do Azure, key1 ou key2.

5. Clique em **Obter depósitos** e, em seguida, selecione um depósito para servir como o destino de transferência.
Após a geração dos depósitos, os campos **Depósito de transferência** e **Depósito de archive** são exibidos.
6. No campo **Depósito de transferência**, selecione um depósito para servir como o destino de transferência.
7. Opcional: No campo **Depósito de archive**, selecione um recurso de armazenamento em nuvem para servir como o destino de archive.
O arquivamento de dados cria uma cópia completa dos dados e pode fornecer benefícios de longo prazo de proteção, custo e segurança. Para obter mais informações sobre como arquivar dados, consulte as informações sobre como copiar dados para o armazenamento de archive em nuvem no [“Transfload para armazenamento de backup secundário” na página 6](#).
8. Clique em **Registrar**.
O armazenamento em nuvem foi incluído na tabela de servidores em nuvem.

O que Fazer Depois

Depois de incluir o armazenamento do Microsoft Azure, conclua a seguinte ação:

Ação	Como
Associar o armazenamento em nuvem à política de ANS que é usada para a tarefa de backup.	Para criar uma política de SLA, consulte “Criando uma política de SLA” na página 89 . Para modificar uma política de ANS existente, consulte “Editando uma política de SLA” na página 93 .

Editando configurações para armazenamento em nuvem

Edite as configurações para um provedor de armazenamento em nuvem para refletir mudanças em seu ambiente de nuvem.

Procedimento

Para editar um provedor de armazenamento em nuvem, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Nuvem**.
2. Clique no ícone editar  que está associado a um provedor em nuvem.
A área de janela **Atualizar nuvem** é exibida.
3. Revise as configurações para o provedor em nuvem e, em seguida, clique em **Atualizar**.

Excluindo o armazenamento em nuvem

Exclua um provedor de armazenamento em nuvem para refletir mudanças em seu ambiente de nuvem. Certifique-se de que o provedor não esteja associado a nenhuma das políticas de ANS antes de excluir o provedor.

Procedimento

Para excluir um provedor de armazenamento em nuvem, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Nuvem**.
2. Clique no ícone excluir  que está associado a um provedor.
3. Clique em **Sim** para excluir o provedor.

Gerenciando o armazenamento do servidor de

É possível transferir para um servidor de repositório para proteção de dados de longo prazo. Para a liberação atual do IBM Spectrum Protect Plus, o servidor do repositório deve ser um Servidor IBM Spectrum Protect Versão 8.1.7 ou mais recente. Para archive em fita, o Servidor IBM Spectrum Protect Versão 8.1.8 ou mais recente é necessário.

Configurando um Servidor IBM Spectrum Protect como um destino de transferência

Para transferir dados para um Servidor IBM Spectrum Protect, deve-se primeiro configurar o IBM Spectrum Protect Plus como um cliente de objeto para o servidor.

Sobre Esta Tarefa

Após a configuração de um cliente de objeto, as chaves e certificado para ativar a conexão segura com o Servidor IBM Spectrum Protect. Esses itens são necessários para incluir o servidor de repositório no IBM Spectrum Protect Plus.

Para incluir o cliente de objeto, você deve estar familiarizado com o ambiente do Servidor IBM Spectrum Protect e ter experiência trabalhando com o Operations Center ou com os comandos administrativos do Servidor IBM Spectrum Protect. Para obter assistência, entre em contato com o administrador do IBM Spectrum Protect.

O IBM Spectrum Protect Plus tem ciência das transferências para o Servidor IBM Spectrum Protect, mas não está ciente das subseqüentes operações de replicação do Servidor IBM Spectrum Protect.

A documentação sobre como configurar o IBM Spectrum Protect como um destino de transferência está disponível no IBM Knowledge Center, conforme a seguir:

- Para obter uma visão geral do processo de configuração, consulte [Transferindo dados do IBM Spectrum Protect Plus](#)
- Para obter os pré-requisitos para o processo de transferência, consulte [Preparando-se para transferir dados do IBM Spectrum Protect Plus](#)
- Para obter informações do sistema operacional AIX, consulte [Configurando para transferir dados em ambientes do AIX®](#)
- Para obter informações do sistema operacional Linux ou Windows, consulte [Configurando para transferir dados em ambientes do Linux e Windows](#)
- Para obter uma visão geral do processo de configuração, consulte [Transferindo dados do IBM Spectrum Protect Plus](#)
- Para obter os pré-requisitos para o processo de transferência, consulte [Preparando-se para transferir dados do IBM Spectrum Protect Plus](#)
- Para obter informações do sistema operacional AIX, consulte [Configurando para transferir dados em ambientes do AIX®](#)
- Para obter informações do sistema operacional Linux ou Windows, consulte [Configurando para transferir dados em ambientes do Linux e Windows](#)

Tarefas relacionadas

“Incluindo um servidor do repositório como um provedor de armazenamento de backup” na página 267
Inclua um servidor do repositório para permitir que o IBM Spectrum Protect Plus transfira dados para o servidor.

Preparando para transferir dados do IBM Spectrum Protect Plus

Antes de transferir dados do IBM Spectrum Protect Plus to IBM Spectrum Protect, conclua as etapas de preparação no ambiente IBM Spectrum Protect.

Procedimento

1. Verifique se é possível abrir uma porta do Servidor IBM Spectrum Protect para o objeto de cliente do IBM Spectrum Protect Plus que você planeja usar para operações de transferência de dados. O

número da porta padrão é 9000. Se houver quaisquer firewalls entre o cliente e o agente de objeto, configure o agente de objeto para acessar a porta apropriada por meio do firewall.

2. Verifique as configurações do domínio de política que você planeja usar para operações de transferência de dados. Um nó cliente de objeto está associado a este domínio de política quando o nó é registrado ou atualizado usando os comandos administrativos do Servidor IBM Spectrum Protect **REGISTER NODE** ou **UPDATE NODE**.

As considerações sobre a especificação de domínios de política para as operações de transferência do IBM Spectrum Protect Plus incluem o seguinte:

- O domínio ao qual o nó está designado deve ter um grupo de cópias de backup. Os objetos que são armazenados em um nó cliente de objeto são sempre objetos de backup. Um grupo de cópias de archive não é necessário.
- Deve-se usar um conjunto de armazenamentos de contêiner. O conjunto de armazenamentos que está especificado no grupo de cópias Copy Destination deve ser um conjunto de armazenamentos de contêiner de diretório ou de contêiner de nuvem.
- Todos os objetos são nomeados com exclusividade. Como não há versões inativas de objetos, é possível configurar o campo Versions Data Exists como 1.
- Os grupos de cópias de backup contêm apenas versões ativas, portanto, é possível configurar os campos Reter versões extras e Reter somente a versão como 0.
- O Servidor IBM Spectrum Protect controla o horário em que os objetos são excluídos. Assegure-se de que o nó do cliente de objeto esteja ativado para permitir a exclusão do grupo de cópias de backup.

Exemplo: Exibir informações detalhadas sobre um domínio de política para uma operação de transferência do IBM Spectrum Protect Plus

Exiba as configurações de um grupo de cópias para um nó cliente de objeto.

```
query copygroup format=detailed
```

```
Policy Domain Name: TAPSRV03_OBJECT
Policy Set Name: SET1
Mgmt Class Name: BACK_DISK
Nome do Grupo de Cópias: STANDARD
Tipo do Grupo de Cópias: Backup
Versions Data Exists: 1
Versions Data Deleted: 0
Retain Extra Versions: 0
Retain Only Version: 0
Modo de Cópia: Modified
Serialização de Cópias: Shared Static
Frequência de Cópias: 0
Copy Destination: DEDUPPOOL
Destino do Índice (TOC):
Last Update by (administrator): JBASIL
Last Update Date/Time: 01/17/2019 14:38:05
Perfil de Gerenciamento:
Changes Pending: No
```

Transando dados para sistemas AIX

É possível transferir dados do IBM Spectrum Protect Plus para um Servidor IBM Spectrum Protect no AIX.

Sobre Esta Tarefa

Um agente de objeto do IBM Spectrum Protect não pode ser executado diretamente em um sistema operacional IBM AIX. No entanto, é possível transferir dados do IBM Spectrum Protect Plus para um cliente de objeto do IBM Spectrum Protect em um sistema AIX, primeiro configurando um agente de objeto em um sistema operacional Linux x86_64. O agente de objeto independente está disponível apenas no sistema operacional Linux x86_64.

Após o cliente de objeto do IBM Spectrum Protect Plus enviar dados para o agente de objeto do IBM Spectrum Protect no Linux x86_64, o agente de objeto transfere dados para um cliente de objeto do IBM Spectrum Protect no AIX.

Procedimento

Para transferir dados do IBM Spectrum Protect Plus para um Servidor IBM Spectrum Protect no AIX, conclua as seguintes etapas:

1. No servidor AIX, emita o seguinte comando administrativo do Servidor IBM Spectrum Protect :

```
setopt EnableAIXS3Interface Yes
```

2. No servidor AIX, defina um agente de objeto emitindo o seguinte comando administrativo do Servidor IBM Spectrum Protect . Para configurar o endereço de alto nível (HLA) e o endereço de baixo nível (LLA), use o endereço IP do sistema host e a porta que o agente de objeto utilizará.

```
definir servidor object_agent_name  
hla=object_agent_host_system_ip_address  
lla=object_agent_port objectagent=yes
```

Dica: O valor padrão para a porta do agente de objeto é 9000. Se um agente de objeto local já estiver em execução no sistema, o agente de objeto que está sendo configurado para o servidor AIX deverá usar um número de porta diferente daquele do agente de objeto existente.

3. Faça download dos seguintes scripts para o sistema host do agente de objeto:

- ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent
- ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/startObjectAgent.sh
- ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc
- ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc.u
- ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/delObjectAgentSvc.sh

O IBM Spectrum Protect Plus ou um Servidor IBM Spectrum Protect pode ser instalado no sistema host do agente de objeto.

Se o Servidor IBM Spectrum Protect estiver instalado, será possível usar o arquivo spObjectAgent no diretório do servidor e não será preciso fazer download do agente e de seus scripts novamente.

4. Assegure-se de que os seguintes arquivos tenham permissões executáveis:

- spObjectAgent
- startObjectAgent.sh
- spObjectAgent.rc
- spObjectAgent.rc.u
- delObjectAgentSvc.sh

5. No sistema do servidor AIX, copie os dois seguintes itens para um diretório no sistema host do agente de objeto no Linux:

- Diretório do servidor do agente de objeto
- Certificado público do servidor

O diretório do servidor do agente de objeto foi criado quando você executou o comando **DEFINE SERVER**. O diretório inclui o arquivo e os certificados a seguir:

- Um arquivo de configuração para criar e iniciar um serviço de agente de objeto
- Certificados para comunicação entre o agente de objeto e o servidor

O diretório do servidor do agente de objeto é criado no diretório de instância do servidor: `/server_instance_home_dir/object_agent_name`. Por exemplo,
`/home/tsminst1/OBJAGENT1`

O certificado público do servidor (`cert256.arm`) está localizado normalmente no diretório de instâncias do servidor.

6. No diretório do servidor do agente de objeto que você copiou na etapa anterior, localize o arquivo de configuração do agente de objeto (`spObjectAgent_objectagentname_serverport.config`).
Por exemplo: `spObjectAgent_OBJAGENT1_1500.config`

No arquivo de configuração, atualize os locais dos arquivos a seguir. Exemplo:

```
objagentexe="/opt/tivoli/tsm/server/bin/spObjectAgent\  
keystore="/home/tsminst1/OBJAGENT1/agentcert.p12"  
pwdfile="/home/tsminst1/OBJAGENT1/agentcert.pwd"  
serverkeypub="/home/tsminst1/OBJAGENT1/cert256.arm"  
agentconfig="/home/tsminst1/OBJAGENT1/spObjectAgent_OBJAGENT1_1500.config"
```

7. Substitua o parâmetro **SERVERHLA** no arquivo de configuração do agente de objeto usando o endereço IP do servidor AIX:

```
serverhla=aix_server_ip_address
```

Dica: O agente de objeto usa este valor para localizar o Servidor IBM Spectrum Protect .

8. Para criar e iniciar o agente de objeto no sistema host, execute o script `startObjectAgent.sh` com o arquivo de configuração:

```
startObjectAgent.sh spObjectAgent_objectagentname_serverport.config
```

9. Registre um cliente do agente de objeto no servidor AIX emitindo o seguinte comando do Servidor IBM Spectrum Protect :

```
nó do registro nodename type=objectclient
```

Importante: Registre o ID do usuário e a senha de login que são gerados automaticamente. Você precisará das credenciais para se conectar ao agente de objeto.

10. Para conectar o cliente de objeto do IBM Spectrum Protect Plus ao agente de objeto, acesse a documentação on-line do IBM Spectrum Protect Plus e siga as instruções em [Incluindo um servidor de repositório como um provedor de armazenamento de backup](#).

Transferindo dados para sistemas Linux e Windows

É possível transferir dados do IBM Spectrum Protect Plus para um Servidor IBM Spectrum Protect no Linux ou Windows.

Procedimento

Para transferir dados do IBM Spectrum Protect Plus para um Servidor IBM Spectrum Protect no Linux ou Windows, conclua as seguintes etapas:

1. Configure um agente de objeto.
 - a) Na barra de menus do Operations Center, clique em **Servidores**.
 - b) Selecione uma linha do servidor e clique em **Detalhes**.
 - c) Selecione **Agente de objeto** na área de janela de navegação esquerda e conclua as etapas para criar um agente de objeto e iniciar um serviço do agente de objeto. Para autenticar-se no agente de objeto, use o certificado que é gerado.

Dica: Como alternativa, use o comando administrativo do Servidor IBM Spectrum Protect , **DEFINE SERVER**, para criar um agente de objeto. Especifique `OBJECTAGENT=YES`. Conclua a configuração iniciando um serviço do agente de objeto no sistema que está hospedando o Servidor IBM Spectrum Protect .

2. Configure um cliente de objeto.

Dica: Se você criar um cliente de objeto antes de criar o agente de objeto correspondente, o assistente Incluir cliente forçará a criação do agente de objeto.

- a) Na barra de menus do Operations Center, clique em **Cientes**.
- b) Na tabela Clientes, clique em **+ Cliente**.
- c) Selecione Cliente de objeto e siga as instruções no assistente **Incluir cliente**.

Depois de concluir o assistente, ele fornece o terminal para comunicação com o agente de objeto no servidor e o ID da chave de acesso e a chave de acesso secreta para se conectar com segurança. Quando o IBM Spectrum Protect Plus é usado como um cliente de objeto, ele deve direcionar suas solicitações para o terminal e deve usar o ID da chave de acesso e a chave de acesso secreta.

Dica: Como alternativa, use o comando **REGISTER NODE** para criar um cliente de objeto. Especifique **TYPE=OBJECTCLIENT**.

Excluindo um serviço do agente de objeto

Quando um agente de objeto for excluído do Servidor IBM Spectrum Protect , o serviço do agente de objeto deverá ser excluído do sistema host. Para concluir o processo de exclusão de um agente de objeto, exclua o serviço correspondente.

Antes de Iniciar

Para excluir o serviço do agente de objeto em um sistema operacional Linux, deve-se executar o script `de10bjectAgentSvc.sh` com o arquivo de configuração do agente de objeto. Assegure-se de que possa efetuar login no sistema host do agente de objeto com o ID do usuário raiz.

Para excluir o serviço do agente de objeto em um sistema operacional Windows, deve-se executar o arquivo em lote `de10bjectAgentSvc.cmd` com o arquivo de configuração do agente de objeto. Assegure-se de que tenha privilégios de administrador do Windows para efetuar logon no sistema host do agente de objeto.

Procedimento

1. Verifique se o agente de objeto foi excluído do Servidor IBM Spectrum Protect emitindo o comando administrativo do servidor **QUERY SERVER**.
2. Abra uma linha de comandos
3. Emita o comando a seguir em uma linha. Os diretórios do servidor padrão são usados nos exemplos.

Linux

```
/opt/tivoli/tsm/server/bin/de10bjectAgentSvc.sh  
/object_agent_config_path/spObjectAgent_objectagentname_server_port.config
```

Windows

```
"C:\Arquivos de Programa\Tivoli\TSM\server\de10bjectAgentSvc.cmd"  
"object_agent_config_path\spObjectAgent_objectagentname_server_port.config"
```

onde:

object_agent_config_path

Especifica o caminho de configuração para o agente de objeto.

objectagentname

Especifica o nome do agente de objeto.

server_port

Especifica o número da porta do Servidor IBM Spectrum Protect .

Incluindo um servidor do repositório como um provedor de armazenamento de backup

Inclua um servidor do repositório para permitir que o IBM Spectrum Protect Plus transfira dados para o servidor.

Antes de Iniciar

Configure a chave e o certificado que são necessários para o servidor do repositório. Para obter instruções, consulte [“Incluindo uma chave de acesso”](#) na página 269 e [“Incluindo um Certificado”](#) na página 269.

Para a liberação atual do IBM Spectrum Protect Plus, o servidor do repositório deve ser um Servidor IBM Spectrum Protect .

Configure o IBM Spectrum Protect Plus como um cliente de objeto para o servidor IBM Spectrum Protect. O nó cliente de objeto transfere e armazena dados transferidos. Depois de concluir o procedimento de configuração, o assistente fornece o terminal para comunicação com o agente de objeto no servidor e o ID de acesso, a chave secreta e o certificado para uma conexão segura. [“Configurando um Servidor IBM Spectrum Protect como um destino de transferência”](#) na página 262.

Os certificados podem ser obtidos no Servidor IBM Spectrum Protect Operations Center, navegando para a seguinte área de janela: **Servidor > Agente de objeto > Certificado de agente**. Como alternativa, o certificado pode ser obtido do dispositivo IBM Spectrum Protect Plus executando o seguinte comando:
`openssl s_client -showcerts -connect <ip-address>:9000 </dev/null 2>/dev/null | openssl x509`

As configurações de retenção de transferência são totalmente controladas por meio de políticas de ANS associadas no IBM Spectrum Protect Plus. As configurações de retenção do grupo de cópia do Servidor IBM Spectrum Protect não são usadas para operações de transferência.

Procedimento

Para incluir um Servidor IBM Spectrum Protect como um provedor de armazenamento de backup, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Servidor do repositório**.
2. Clique em **Incluir servidor do repositório**.
3. Preencha os campos na área de janela **Registrar servidor do repositório**:

Nome

Insira um nome significativo para ajudar a identificar o servidor do repositório.

Hostname

Insira o endereço de alto nível (HLA) do agente de objeto do servidor de repositório. Executando o comando `q sev OBJAGENT f=d` do IBM Spectrum Protect, é possível recuperar essas informações.

Porta

Insira a porta de comunicações do servidor do repositório.

Utilizar a chave existente

Ative para selecionar uma chave inserida anteriormente para o repositório e, em seguida, selecione a chave da lista **Selecionar uma chave**.

Se você não selecionar esta opção, preencha os seguintes campos para incluir uma chave:

Nome principal

Insira um nome significativo para ajudar a identificar a chave.

Chave de acesso

Insira a chave de acesso.

Chave secreta

Insira a chave secreta.

Certificado

Selecione um método de associação de um certificado com o recurso. Se estiver copiando o certificado, as linhas de texto BEGIN e END deverão ser incluídas.

Fazer Upload

Selecione e clique em **Procurar** para localizar o certificado e, em seguida, clique em **Fazer upload**.

Copiar e colar

Selecione para inserir o nome do certificado, copiar e colar os conteúdos do certificado, em seguida, clique em **Criar**.

Utilizar existente

Selecione para usar um certificado transferido por upload anteriormente.

4. Clique em **Registrar**.

O servidor IBM Spectrum Protect é incluído na tabela de servidores de repositório.

O que Fazer Depois

Depois de incluir um servidor do repositório, conclua a seguinte ação:

Ação	Como
Associe o servidor do repositório à política de ANS que é usada para a tarefa de backup.	Para criar uma política de SLA, consulte “Criando uma política de SLA” na página 89. Para modificar uma política de ANS existente, consulte “Editando uma política de SLA” na página 93.

Editando Configurações para um Servidor de Repositório

Edite as configurações para um provedor de servidor do repositório para refletir mudanças em seu ambiente de nuvem.

Procedimento

Para editar um provedor do servidor de repositório, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Servidor do repositório**.
2. Clique no ícone editar  que está associado a um provedor de servidor do repositório. A área de janela **Atualizar servidor do repositório** é exibida.
3. Revise as configurações para o provedor de servidor do repositório e, em seguida, clique em **Atualizar**.

Excluindo um servidor de repositório

Exclua um provedor de servidor do repositório para refletir mudanças em seu ambiente. Certifique-se de que o provedor não esteja associado a nenhuma das políticas de ANS antes de excluir o provedor.

Procedimento

Para excluir um provedor de servidor do repositório, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Servidor do repositório**.
2. Clique no ícone excluir  que está associado a um provedor de servidor do repositório.
3. Clique em **Sim** para excluir o provedor.

Gerenciando Chaves e Certificados

Os recursos em nuvem e os servidores de repositório requerem credenciais para servir como destinos de transferência. As chaves de acesso e as chaves secretas são fornecidas por seu recurso em nuvem ou

interface do servidor de repositório. Essas chaves servem como o nome de usuário e a senha de seus destinos de transferência e permitem que eles sejam acessados pelo IBM Spectrum Protect Plus. Alguns destinos de transferência também requerem certificados para a segurança de dados adicional.

Ao utilizar um recurso no IBM Spectrum Protect Plus que requer credenciais para acessar um destino de transferência, selecione **Usar chave existente** ou **Usar certificado existente** e selecione a chave ou certificado associado.

Incluindo uma chave de acesso

Inclua uma chave de acesso para fornecer credenciais do servidor em nuvem ou do servidor do repositório.

Procedimento

Para incluir uma chave, conclua as seguintes etapas:

1. Crie sua chave de acesso e chave secreta por meio da interface do recurso em nuvem ou do servidor do repositório. Anote a chave de acesso e a chave secreta.
2. No menu de navegação, clique em **Configuração do sistema > Chaves e certificados**.
3. Na seção **Chaves de acesso**, clique em **Incluir chave de acesso**.
4. Preencha os campos na área de janela **Propriedades da chave**:

Nome

Insira um nome significativo para ajudar a identificar a chave de acesso.

Chave de Acesso

Insira a chave de acesso do recurso em nuvem ou do servidor do repositório. Para o Microsoft Azure, insira o nome da conta de armazenamento.

Chave Secreta

Insira a chave secreta do recurso em nuvem ou do servidor do repositório. Para o Microsoft Azure, insira a chave a partir de um dos campos-chave, key1 ou key2.

5. Clique em **Salvar**.

A chave é exibida na tabela **Chaves de acesso** e pode ser selecionada ao utilizar um recurso que requer credenciais para acessar um recurso por meio da opção **Usar chave existente**.

Excluindo uma chave de acesso

Exclua uma chave de acesso quando ela se tornar obsoleta. Certifique-se de redesignar uma nova chave de acesso a seu recurso em nuvem ou servidor do repositório.

Procedimento

Para excluir uma chave de acesso, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Chaves e certificados**.
2. Clique no ícone excluir  que está associado a uma chave de acesso.
3. Clique em **Sim** para excluir a chave de acesso.

Incluindo um Certificado

Inclua um certificado para fornecer credenciais do servidor de recurso em nuvem ou de repositório.

Procedimento

Para incluir um certificado, conclua as seguintes etapas:

1. Exporte um certificado de seu servidor de recurso em nuvem ou de repositório.
2. No menu de navegação, clique em **Configuração do sistema > Chaves e certificados**.
3. Na seção **Certificados**, clique em **Incluir certificado**.
4. Preencha os campos na área de janela **Propriedades do certificado**:

Tipo

Selecione o tipo de servidor de recurso em nuvem ou de repositório.

Certificado

Selecione um método para incluir o certificado:

Fazer Upload

Selecione para procurar o certificado localmente.

Copiar e colar

Selecione para inserir o nome do certificado e copiar e colar o conteúdo do certificado.

5. Clique em **Salvar**.

A chave é exibida na tabela **Certificados** e pode ser selecionada ao utilizar um recurso que requer credenciais para acessar um recurso por meio da opção **Usar certificado existente**.

Excluindo um Certificado

Exclua um certificado quando ele se tornar obsoleto. Certifique-se de redesignar um novo certificado a seu recurso em nuvem ou servidor do repositório.

Procedimento

Para excluir um certificado, conclua as etapas a seguir:

1. No menu de navegação, clique em **Configuração do sistema > Chaves e certificados**.
2. Clique no ícone excluir  que está associado a um certificado.
3. Clique em **Sim** para excluir o certificado.

Incluindo uma chave SSH

Inclua uma chave SSH para fornecer credenciais para recursos baseados no Linux, incluindo operações de indexação e restauração de arquivos em máquinas virtuais no vCenter e Hyper-V, bem como em servidores de aplicativos Oracle, Db2 e MongoDB. As chaves SSH fornecem uma conexão segura entre seus recursos e o IBM Spectrum Protect Plus.

Antes de Iniciar

- O serviço SSH deve estar em execução na porta 22 no servidor e todos os firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor usando SSH. O subsistema SFTP para SSH também deve estar ativado.
- Certifique-se de que a chave SSH pública seja colocada em um arquivo `authorized_keys` apropriado para o usuário do agente do IBM Spectrum Protect Plus. Geralmente, o arquivo está localizado em `/home/<username>/.ssh/authorized_keys`. O diretório `.ssh` e todos os arquivos contidos nele devem ter suas permissões configuradas para 600.

Procedimento

Para incluir uma chave, conclua as seguintes etapas:

1. Em seu recurso, gere uma chave SSH. Por exemplo, em um servidor Oracle, insira o comando `ssh-keygen` e siga as instruções.
2. Quando solicitado a **Inserir arquivo** no qual salvar a chave, insira um arquivo e local, por exemplo: `/root/sshkey`.
3. No local `/root` no servidor inserido na etapa 2, o arquivo `sshkey.pub` contém a chave pública. Posteriormente, isso será copiado, colado e salvo no arquivo `authorized_keys` após a execução de `cd ~/.ssh` enquanto estiver com login efetuado como o usuário designado ao IBM Spectrum Protect Plus
4. Na área de janela de navegação do IBM Spectrum Protect Plus, clique em **Configuração do sistema > Chaves e certificados**.
5. Na seção **Chaves SSH**, clique em **Incluir chave SSH**.

6. Preencha os campos na área de janela **Propriedades da chave SSH**:

Nome

Insira um nome significativo para ajudar a identificar a chave SSH.

Usuário

Insira o usuário associado ao recurso e à chave SSH.

Chave Privada

Copie e cole a chave privada, que pode ser localizada no arquivo sshkey.

7. Clique em **Salvar**.

A chave é exibida na tabela **Chaves SSH** e pode ser selecionada ao utilizar um recurso que requer credenciais para acessar um recurso por meio da opção **Chave**.

Excluindo uma chave SSH

Exclua uma chave SSH quando ela se tornar obsoleta. Certifique-se de redesignar uma nova chave SSH a seus recursos.

Procedimento

Para excluir uma chave SSH, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > Chaves e certificados**.
2. Clique no ícone excluir  que está associado a uma chave SSH.
3. Clique em **Sim** para excluir a chave de acesso.

Gerenciando sites

Um *site* é uma construção de política do IBM Spectrum Protect Plus que é usada para gerenciar o posicionamento de dados em um ambiente.

Um site pode ser físico, como um data center, ou lógico, como um departamento ou organização. Os componentes do IBM Spectrum Protect Plus são designados a sites para localizar e otimizar caminhos de dados. Uma implementação do IBM Spectrum Protect Plus sempre tem pelo menos um site por local físico.

Por padrão, o ambiente do IBM Spectrum Protect Plus tem um site primário, um site secundário e um site de demonstração.

Incluindo um Site

Depois de incluir um site no IBM Spectrum Protect Plus, é possível designar servidores de armazenamento de backup ao site.

Procedimento

Para incluir um site, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Site**.
2. Clique em **Incluir Site**.
A área de janela **Propriedades do Site** é exibida.
3. Insira um nome de site.
4. Opcional: Para gerenciar a atividade de rede em um planejamento definido, mude o rendimento para operações de replicação e transferência de site:
 - a) Marque a caixa de seleção **Ativar regulador**.
 - b) No campo **Taxa**, ajuste o rendimento:
 - 1) Mude a taxa numérica do rendimento, clicando nas setas para cima ou para baixo.

2) Selecione uma unidade para o rendimento. As opções incluem **bytes/s**, **KB/s**, **MB/s** e **GB/s**. O rendimento padrão é de 100 MB/s (megabytes por segundo).

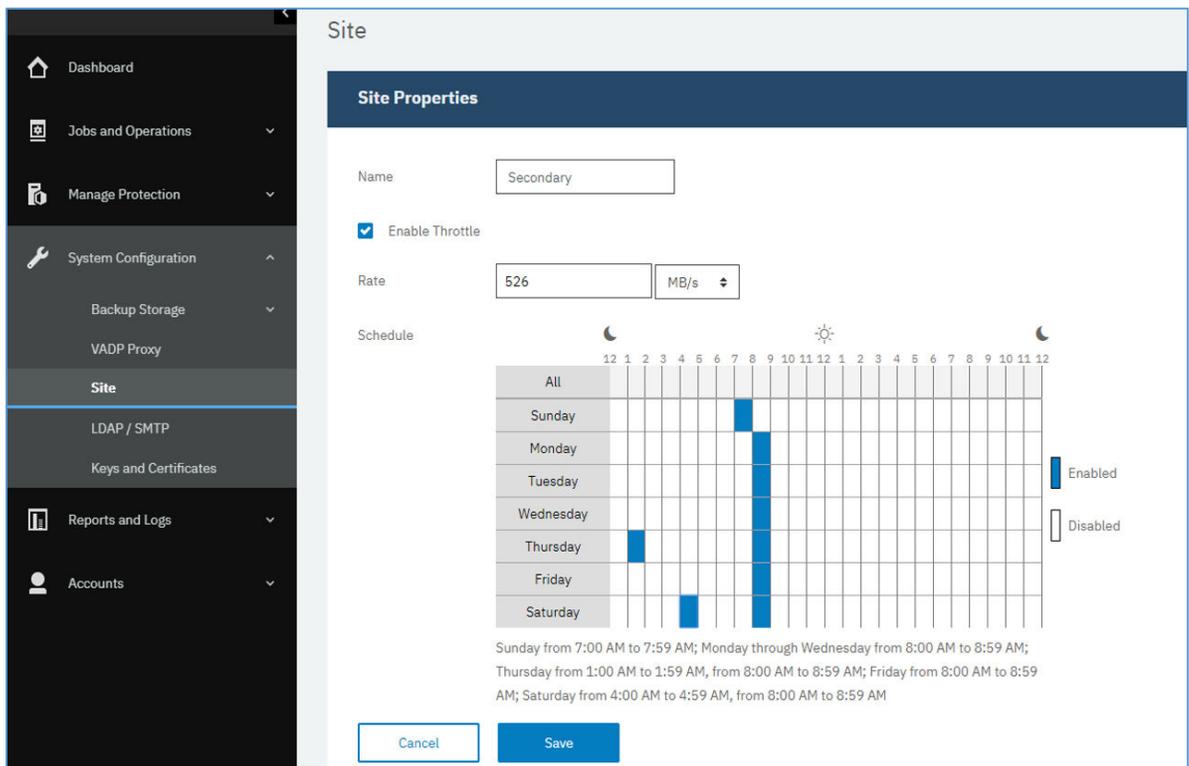


Figura 30. Ativando diferentes taxas de limitação para diferentes horários para melhorar o rendimento

c) Na tabela de planejamento semanal, selecione horários diários para limitação ou selecione dias e horários específicos para limitação.

Dica: Para selecionar um horário, clique em um intervalo de tempo na tabela. O intervalo de tempo selecionado é destacado. Para limpar um intervalo de tempo, clique em um intervalo de tempo destacado. Para selecionar o mesmo intervalo de tempo para cada dia da semana, clique em um intervalo de tempo na linha **Todos**.

Depois de fazer suas seleções, os dias e horários de limitação são listados abaixo da tabela de planejamento.

5. Clique em **Salvar** para confirmar as mudanças e fechar a área de janela.

Resultados

O site é exibido na tabela de sites e pode ser aplicado a servidores de armazenamento de backup novos e existentes.

Editando um Site

Revise as informações do site para refletir as mudanças em seu ambiente do IBM Spectrum Protect Plus.

Procedimento

Para editar um site, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Site**.
2. Clique no ícone editar  que está associado a um site.
A área de janela **Propriedades do Site** é exibida.
3. Revise o nome do site.

4. Opcional: Para gerenciar a atividade de rede em um planejamento definido, mude o rendimento para operações de replicação e transferência de site:
- Marque a caixa de seleção **Ativar regulador**.
 - No campo **Taxa**, ajuste o rendimento:
 - Mude a taxa numérica do rendimento, clicando nas setas para cima ou para baixo.
 - Selecione uma unidade para o rendimento. As opções incluem **bytes/s**, **KB/s**, **MB/s** e **GB/s**.
O rendimento padrão é de 100 MB/s (megabytes por segundo).

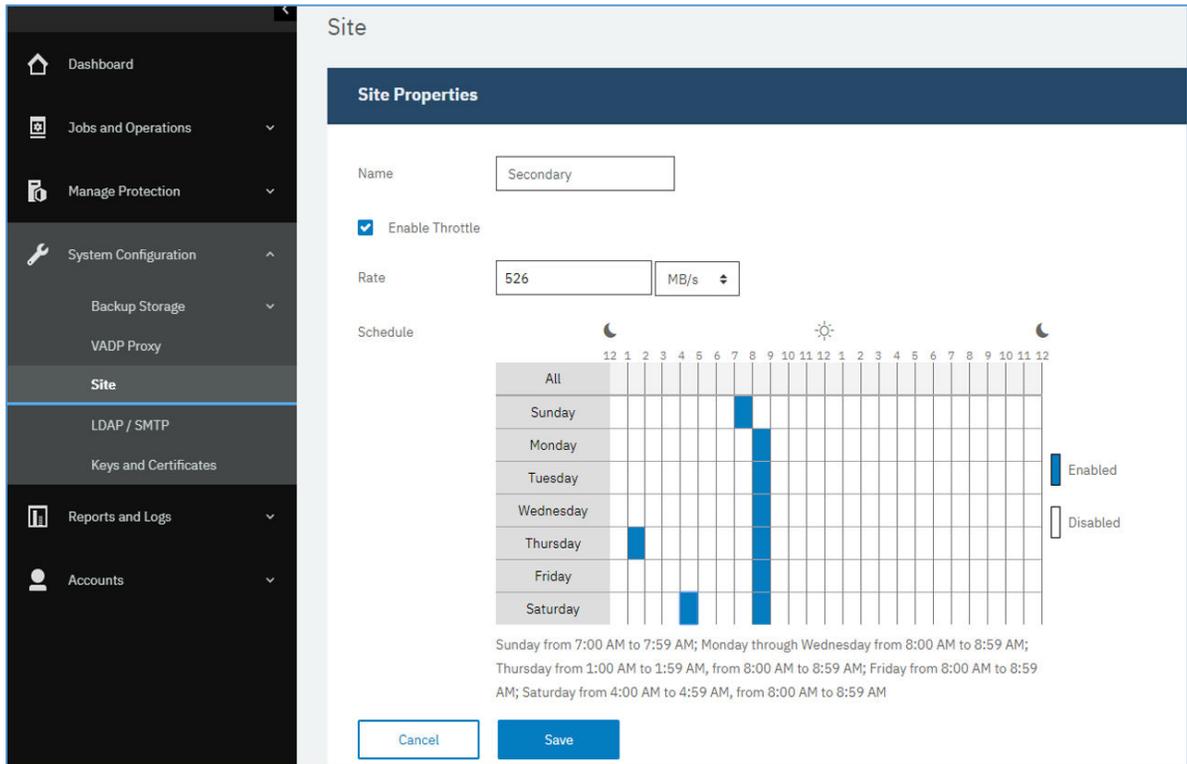


Figura 31. Ativando diferentes taxas de limitação para diferentes horários para melhorar o rendimento

- Na tabela de planejamento semanal, selecione horários diários para limitação ou selecione dias e horários específicos para limitação.

Dica: Para selecionar um horário, clique em um intervalo de tempo na tabela. O intervalo de tempo selecionado é destacado. Para limpar um intervalo de tempo, clique em um intervalo de tempo destacado. Para selecionar o mesmo intervalo de tempo para cada dia da semana, clique em um intervalo de tempo na linha **Todos**.

Depois de fazer suas seleções, os dias e horários de limitação são listados abaixo da tabela de planejamento.

- Clique em **Salvar** para confirmar as mudanças e fechar a área de janela.

Excluindo um Site

Exclua um site quando ele se tornar obsoleto. Certifique-se de redesignar seu armazenamento de backup a sites diferentes antes de excluir o site.

Procedimento

Para excluir um site, conclua as seguintes etapas:

- Na área de janela de navegação, clique em **Configuração do sistema > Site**.
- Clique no ícone excluir **X** que está associado a um site.

3. Clique em **Sim** para excluir o site.

Gerenciando servidores LDAP e SMTP

É possível incluir um Lightweight Directory Access Protocol (LDAP) e um servidor de Protocolo Simples de Transporte de Correio (SMTP) para uso no IBM Spectrum Protect Plus para uso em recursos de conta do usuário e de relatório.

Tarefas relacionadas

“Criando uma conta do usuário para um grupo LDAP” na página 306

Inclua uma conta do usuário para um grupo LDAP no IBM Spectrum Protect Plus.

“Planejando um relatório” na página 294

É possível planejar relatórios customizados no IBM Spectrum Protect Plus para execução em horários específicos.

Incluindo um servidor LDAP

Deve-se incluir um servidor LDAP para criar contas do usuário do IBM Spectrum Protect Plus usando um grupo LDAP. Essas contas permitem que os usuários acessem o IBM Spectrum Protect Plus usando nomes de usuário e senhas LDAP. Apenas um servidor LDAP pode ser associado a uma instância do dispositivo virtual IBM Spectrum Protect Plus.

Sobre Esta Tarefa

É possível incluir um servidor Microsoft Active Directory ou OpenLDAP. Observe que o OpenLDAP não suporta o filtro de usuário sAMAaccountName que é comumente usado com o Active Directory. Além disso, a opção **memberOf** deve estar ativada no servidor OpenLDAP.

Procedimento

Para registrar um servidor LDAP, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > LDAP/SMTP**.
2. Na área de janela **Servidores LDAP**, clique em **Incluir servidor LDAP**.
3. Preencha os seguintes campos na área de janela **Servidores LDAP**:

Endereço do Host

O endereço IP do host ou nome lógico do servidor LDAP.

Porta

A porta na qual o servidor LDAP está atendendo. A porta padrão típica é 389 para conexões não SSL ou 636 para conexões SSL.

SSL

Ative a opção SSL para estabelecer uma conexão segura com o servidor LDAP.

Utilizar usuário existente

Ative para selecionar um nome de usuário e senha inseridos anteriormente para o servidor LDAP.

Nome de ligação

O nome distinto de ligação que é usado para autenticar a conexão com o servidor LDAP. IBM Spectrum Protect Plus suporta a ligação simples.

Password

A senha que está associada com o Nome Distinto da Ligação.

DN base

O local em que os usuários e grupos podem ser localizados.

Filtro de usuário

Um filtro para selecionar apenas os usuários no DN Base que correspondem a determinados critérios. Um exemplo de um filtro de usuário padrão válido é `cn={0}`.

Dicas:

- Para ativar a autenticação usando o atributo de nomenclatura do usuário do Windows **sAMAccountName**, configure o filtro como `samaccountname={0}`. Quando este filtro está configurado, os usuários efetuam login no IBM Spectrum Protect Plus usando apenas um nome de usuário. Um domínio não está incluído.
- Para ativar a autenticação usando o atributo de nomenclatura do nome do principal do usuário (UPN), configure o filtro como `userprincipalname={0}`. Quando este filtro está configurado, os usuários efetuam login no IBM Spectrum Protect Plus usando o formato `username@domain`.
- Para ativar a autenticação usando um endereço de e-mail que está associado ao LDAP, configure o filtro como `mail={0}`.

A configuração de **Filtro de usuário** também controla o tipo de nome do usuário que aparece na exibição de usuários do IBM Spectrum Protect Plus.

RDN do Usuário

O caminho distinto relativo para o usuário. Especifique o caminho no qual os registros do usuário podem ser localizados. Um exemplo de um RDN padrão válido é `cn=Users`.

RDN de Grupo

O caminho distinto relativo para o grupo. Se o grupo estiver em um nível diferente do caminho do usuário, especifique o caminho em que os registros do grupo podem ser localizados.

4. Clique em **Salvar**.

Resultados

IBM Spectrum Protect Plus conclui as ações a seguir:

1. Confirma que foi feita uma conexão de rede.
2. Inclui o servidor LDAP no banco de dados.

Depois que o servidor SMTP for incluído, o botão **Incluir servidor LDAP** não estará mais disponível.

O que Fazer Depois

Se for retornada uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se suas entradas estiverem corretas e a conexão for malsucedida, entre em contato com um administrador da rede para revisar as conexões.

Tarefas relacionadas

[“Criando uma conta do usuário para um grupo LDAP” na página 306](#)

Inclua uma conta do usuário para um grupo LDAP no IBM Spectrum Protect Plus.

Incluindo um servidor SMTP

Deve-se incluir um servidor SMTP para enviar relatórios planejados para destinatários de e-mail. Apenas um servidor SMTP pode ser associado a um dispositivo virtual IBM Spectrum Protect Plus.

Procedimento

Para incluir um servidor SMTP, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > LDAP/SMTP**.
2. Na área de janela **Servidores SMTP**, clique em **Incluir servidor SMTP**.
3. Preencha os seguintes campos na área de janela **Servidores SMTP**:

Endereço do Host

O endereço IP do host, ou o caminho e nome do host do servidor SMTP.

Porta

A porta de comunicações do servidor que está sendo incluído. A porta padrão típica é 25 para conexões não SSL ou 443 para conexões SSL.

Nome de Usuário

O nome que é usado para acessar o servidor SMTP.

Password

A senha associada ao nome de usuário.

Tempo Limite

O valor de tempo limite de email em milissegundos.

De Endereço

O endereço que está associado a comunicações por e-mail do IBM Spectrum Protect Plus.

Prefixo do Assunto

O prefixo a ser incluído nas linhas de assunto de e-mail enviadas do IBM Spectrum Protect Plus.

4. Clique em **Salvar**.

Resultados

IBM Spectrum Protect Plus conclui as ações a seguir:

1. Confirma que foi feita uma conexão de rede.
2. Inclui o servidor no banco de dados.

Se for retornada uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se suas entradas estiverem corretas e a conexão for malsucedida, entre em contato com um administrador da rede para revisar as conexões.

Para testar a conexão SMTP, clique no botão **Testar servidor SMTP** e, em seguida, insira um endereço de e-mail. Clique em **Enviar**. Uma mensagem de e-mail de teste é enviada para o endereço de e-mail para verificar a conexão.

Depois que o servidor SMTP for incluído, o botão **Incluir servidor SMTP** não estará mais disponível.

O que Fazer Depois

Tarefas relacionadas

[“Planejando um relatório” na página 294](#)

É possível planejar relatórios customizados no IBM Spectrum Protect Plus para execução em horários específicos.

Editando configurações para um servidor LDAP ou SMTP

Edite as configurações para um servidor LDAP ou SMTP para refletir mudanças no ambiente IBM Spectrum Protect Plus.

Procedimento

Para editar as configurações para um servidor LDAP ou SMTP, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > LDAP/SMTP**.
2. Clique no ícone editar  que está associado ao servidor.
A área de janela de edição é exibida.
3. Revise as configurações para o servidor e, em seguida, clique em **Salvar**.

Excluindo um servidor LDAP ou SMTP

Exclua um servidor LDAP ou SMTP quando ele se tornar obsoleto. Certifique-se de que o servidor não esteja em uso pelo IBM Spectrum Protect Plus antes de excluí-lo.

Procedimento

Para excluir um servidor LDAP ou SMTP, conclua as seguintes etapas:

1. No menu de navegação, clique em **Configuração do sistema > LDAP/SMTP**.
2. Clique no ícone excluir  que está associado ao servidor.
3. Clique em **Sim** para excluir o servidor.

Aplicando preferências globais

Como administrador, é possível gerenciar preferências que se aplicam a todas as operações do IBM Spectrum Protect Plus na área de janela **Preferências globais**.

Antes de Iniciar

Apenas o usuário com credenciais de administrador pode gerenciar as preferências globais.

Sobre Esta Tarefa

A área de janela **Preferências globais** contém valores padrão para parâmetros que se aplicam a todas as operações do IBM Spectrum Protect Plus. As preferências são organizadas em três categorias: aplicativo, proteção e segurança.

Os valores padrão para as preferências globais são mostrados na tabela a seguir.

Preferências	Valor padrão	Unidade (se aplicável)
Servidores de aplicativo simultâneos para sessões de backup	0	
Porcentagem de avisos livres do vSnap (%)	30	Porcentagem (%)
Porcentagem de erro livre do vSnap (%)	20	Porcentagem (%)
Agrupar VMs por tamanho do grupo de VMs (GB)	5120	Gigabytes
Agrupar VMs por número de VMs no grupo	20	
Tempo limite de conexão do VMware	300	Segundos
Intervalo de atualização de backup	300	Segundos
Comprimento Mínimo da Senha	8	Caracteres

É possível alterar os valores padrão na área de janela **Preferências globais**.

Procedimento

1. Na área de janela de navegação, clique em **Configuração do sistema > Preferências globais**.
2. Atualize os valores para as preferências globais. Para reverter para o valor padrão a partir de um valor inserido anteriormente, clique no ícone de reconfiguração .

Preferências	Descrição
Aplicativo	Servidores de aplicativo simultâneos para sessões de backup O número máximo de servidores de aplicativos simultâneos por sessão de backup.
Backup (Hypervisor / Aplicativo)	Porcentagem de avisos livres do vSnap (%) O limite de porcentagem de espaço livre restante no conjunto de armazenamentos vSnap. Os avisos são exibidos no log da tarefa. Por exemplo, se um valor 10 for especificado, um aviso será exibido se o conjunto de armazenamentos vSnap tiver 10% ou menos de espaço livre restante. Porcentagem de erro livre do vSnap (%) O limite de porcentagem de espaço livre restante no conjunto de armazenamentos vSnap. Os erros são exibidos no log da tarefa. Por exemplo, se um valor 5 for especificado, um erro será exibido se o conjunto de armazenamentos vSnap tiver 5% ou menos de espaço livre restante.
Hypervisor	MVs de grupo As máquinas virtuais podem ser agrupadas. O grupo pode ser definido por uma contagem dos MVs contidos ou pelo tamanho das MVs contidas no grupo. Tempo limite de conexão do VMware O período de tempo em que o IBM Spectrum Protect Plus espera pela conclusão de comandos que são emitidos para os vCenters conectados. Se as operações não forem concluídas dentro do período de tempo especificado, elas serão registradas como erros. Essa configuração se aplica apenas aos hypervisores VMware. Intervalo de atualização de backup A frequência em que as mensagens sobre o progresso da transferência de dados são atualizadas no log da tarefa.
Segurança	Comprimento Mínimo da Senha O comprimento mínimo das senhas para o IBM Spectrum Protect Plus. Por padrão, a senha tem um comprimento mínimo de 8 caracteres, mas é possível especificar uma senha maior. Esse valor se aplica a todas as contas do usuário.

Nota: Para o Agrupamento de VM, há quatro grupos de VMs e cada grupo de VMs pode ter um máximo de cinco VMs. Cada grupo corresponde a um volume de destino (fluxo de dados). Um máximo de 20 VMs (4 fluxos de dados) pode ser feito em um tempo baseado em cálculos de tamanho.

Efetando Logon no Console Administrativo

Efetue logon no console administrativo para revisar a configuração do dispositivo virtual IBM Spectrum Protect Plus. As informações disponíveis incluem configurações gerais do sistema, configurações de rede e de proxy.

Procedimento

Para efetuar logon no console administrativo, conclua as seguintes etapas:

1. Em um navegador suportado, insira a seguinte URL:

```
https://HOSTNAME:8090/
```

Em que *HOSTNAME* é o endereço IP da máquina virtual na qual o aplicativo é implementado.

2. Na janela de login, selecione um dos seguintes tipos de autenticação na lista **Tipo de autenticação**:

Tipo de Autenticação	Informações de Logon
IBM Spectrum Protect Plus	Para efetuar logon como um usuário do IBM Spectrum Protect Plus com privilégios SYSADMIN, insira seu nome de usuário e senha de administrador.
System	Para efetuar logon como um usuário do sistema, insira a senha <code>serveradmin</code> . A senha padrão é <code>sppDP758</code> . É solicitado que mude esta senha durante o primeiro logon.

O que Fazer Depois

Revise a configuração do dispositivo virtual IBM Spectrum Protect Plus.

Conceitos relacionados

“Requisitos de Sistema” na página 11

Antes de instalar o IBM Spectrum Protect Plus, revise os requisitos de hardware e de software para o produto e outros componentes que você planeja instalar no ambiente de armazenamento.

“Gerenciando atribuições” na página 301

As funções definem as ações que podem ser concluídas para os recursos que são definidos em um grupo de recursos. Enquanto um grupo de recursos define os recursos que estão disponíveis para uma conta, uma função configura as permissões para interagir com os recursos.

Configurando o fuso horário

Use o Console Administrativo para configurar o fuso horário do dispositivo IBM Spectrum Protect Plus.

Procedimento

Para configurar o fuso horário, conclua as seguintes etapas:

1. Em um navegador suportado, insira a seguinte URL:

```
https://HOSTNAME:8090/
```

Em que *HOSTNAME* é o endereço IP da máquina virtual na qual o aplicativo é implementado.

2. Na janela de login, selecione um dos seguintes tipos de autenticação na lista **Tipo de autenticação**:

Tipo de Autenticação	Informações de login
IBM Spectrum Protect Plus	Para efetuar login como um usuário do IBM Spectrum Protect Plus com privilégios SYSADMIN, insira seu nome de usuário e senha de administrador.
System	Para efetuar login como um usuário do sistema, insira a senha <code>serveradmin</code> . A senha padrão é <code>sppDP758</code> . É solicitado que mude esta senha durante o primeiro login.

3. Clique em **Executar Ações do Sistema** .
4. Na seção **Mudar fuso horário**, selecione seu fuso horário.
É exibida uma mensagem informando que a operação foi bem-sucedida. Todos os logs e planejamentos do IBM Spectrum Protect Plus refletirão o fuso horário selecionado. O fuso horário selecionado também será exibido no dispositivo IBM Spectrum Protect Plus quando tiver com login efetuado com o ID do usuário **serveradmin**.
5. Para visualizar o fuso horário atual, selecione **Informações do produto** da página principal do Console Administrativo.

Fazendo upload de um certificado SSL a partir do console administrativo

Para estabelecer conexões seguras no IBM Spectrum Protect Plus, é possível fazer upload de um certificado SSL, como um certificado HTTPS ou LDAP usando o console administrativo.

Sobre Esta Tarefa

Para certificados HTTPS, os certificados codificados por PEM com extensões `.cer` ou `.crt` são suportados.

Para certificados LDAP/Hyper-V, os certificados codificados por DER com extensões `.cer` ou `.crt` são suportados. Se estiver fazendo upload de um certificado SSL LDAP, certifique-se de que o IBM Spectrum Protect Plus tenha conectividade com o servidor LDAP e que o servidor LDAP esteja em execução.

Os certificados de formatos ASCII e binário são aceitos com as extensões de arquivo padrão `.pem`, `.cer` e `.crt`. No entanto, a função de importação de certificado do console administrativo não pode ser usada para atualizar as comunicações do servidor da web SSL do dispositivo. Para fazer upload de certificados de formatos ASCII e binário, use a linha de comandos conforme descrito em [“Fazendo upload de um certificado SSL a partir da linha de comandos”](#) na página 281

Procedimento

Para fazer upload de um certificado SSL, conclua as seguintes etapas:

1. Entre em contato com o administrador da rede para saber o nome do certificado a ser exportado.
2. Em um navegador suportado, exporte o certificado para seu computador. Anote o local do certificado em seu computador. O processo de exportação de certificados varia com base em seu navegador.
3. Em um navegador suportado, insira a seguinte URL:

```
https://HOSTNAME:8090/
```

Em que *HOSTNAME* é o endereço IP da máquina virtual na qual o aplicativo é implementado.

4. Na janela de logon, selecione um dos seguintes tipos de autenticação na lista **Tipo de autenticação** :

Tipo de Autenticação	Informações de Logon
IBM Spectrum Protect Plus	Para efetuar logon como um usuário do IBM Spectrum Protect Plus com privilégios SYSADMIN, insira seu nome de usuário e senha de administrador.
System	Para efetuar logon como um usuário do sistema, insira a senha <code>serveradmin</code> . A senha padrão é <code>sppDP758</code> . É solicitado que mude esta senha durante o primeiro logon.

5. Clique em **Gerenciar seus certificados** .
6. Clique em **Procurar** e selecione o certificado que você deseja transferir por upload.
7. Clique em **Fazer Upload de Certificado SSL para HTTPS** .

8. Reinicie a máquina virtual na qual o aplicativo está implementado.

Fazendo upload de um certificado SSL a partir da linha de comandos

Para fazer upload de certificados de formatos ASCII e binário, use a linha de comandos para o dispositivo virtual IBM Spectrum Protect Plus. Os certificados são aceitos com as extensões de arquivo padrão `.pem`, `.cer` e `.crt`.

Sobre Esta Tarefa

Este processo requer que você compacte a chave privada, a chave pública e certificados em cadeia em um formato de arquivo PKCS12 (geralmente referido como arquivo PFX com a extensão `.p12`) e importe isso manualmente para o Java keystore do IBM Spectrum Protect Plus. O procedimento considera que você já tenha os objetos de segurança privados, públicos e todos os de suporte oferecidos pelo fornecedor de segurança, compactados em um formato de arquivo PKCS12 chamado *name*.p12.

Se você não tiver esse arquivo, deve trabalhar com seu fornecedor de segurança usando um servidor separado e/ou OpenSSL para gerar a solicitação de assinatura de certificado necessária. Depois de receber, compacte os objetos privados, públicos e de certificado em cadeia resultantes no arquivo necessário referenciado abaixo.

Procedimento

Para importar o arquivo *name*.p12, conclua as seguintes etapas:

1. Efetue logon com o ID do usuário **serveradmin** no dispositivo virtual IBM Spectrum Protect Plus.

A senha inicial é `sppDP758`.

2. Na linha de comandos, execute o seguinte comando:

```
/usr/java/latest/bin/keytool -importkeystore -deststorepass ecx-beta -  
destkeystore /opt/virgo/configuration/keystore -srckeystore NAME.p12 -  
srcstoretype PKCS12
```

3. Reinicie o dispositivo virtual.

Efetuando logon no dispositivo virtual

Efetue logon no dispositivo virtual IBM Spectrum Protect Plus usando o vSphere Client para acessar a linha de comandos. É possível acessar a linha de comandos em um ambiente VMware ou em um ambiente Hyper-V.

Acessando o dispositivo virtual no VMware

Em um ambiente VMware, efetue logon no dispositivo virtual IBM Spectrum Protect Plus por meio do vSphere Client para acessar a linha de comandos.

Procedimento

Conclua as seguintes etapas para acessar a linha de comandos do dispositivo virtual:

1. No vSphere Client, selecione a máquina virtual na qual o IBM Spectrum Protect Plus está implementado.

2. Na guia **Resumo**, selecione **Abrir Console** e clique no console.

3. Selecione **Efetuar login** e insira seu nome de usuário e senha. O nome do usuário padrão é `serveradmin` e a senha padrão é `sppDP758`.

O que Fazer Depois

Insira comandos para administrar o dispositivo virtual. Para efetuar logoff, digite `exit`.

Acessando o dispositivo virtual no Hyper-V

Em um ambiente Hyper-V, efetue login no dispositivo virtual IBM Spectrum Protect Plus por meio do vSphere Client para acessar a linha de comandos.

Procedimento

Conclua as seguintes etapas para acessar a linha de comandos do dispositivo virtual:

1. No Hyper-V Manager, selecione a máquina virtual na qual o IBM Spectrum Protect Plus está implementado.
2. Clique com o botão direito na máquina virtual e selecione **Conectar**.
3. Selecione **Efetuar login** e insira seu nome de usuário e senha. O nome do usuário padrão é `serveradmin` e a senha padrão é `sppDP758`.

O que Fazer Depois

Insira comandos para administrar o dispositivo virtual. Para efetuar logoff, digite `exit` .

Testando a conectividade de rede

A Ferramenta de Serviço do IBM Spectrum Protect Plus testa endereços e portas do host para determinar se uma conexão pode ser estabelecida. É possível usar a Ferramenta de Serviço para verificar se uma conexão pode ser estabelecida entre o IBM Spectrum Protect Plus e um nó

É possível executar a Ferramenta de Serviço a partir da linha de comandos do IBM Spectrum Protect Plus ou remotamente usando um arquivo `.jar`. Se uma conexão puder ser estabelecida, a ferramenta retornará um visto verde. Se uma conexão não puder ser estabelecida, a condição de erro será exibida, junto com possíveis causas e ações.

A ferramenta fornece orientação para as seguintes condições de erro:

- Tempo limite
- Conexão recusada
- Host desconhecido
- Nenhuma rota

Executando a Ferramenta de Serviço a partir de uma interface da linha de comandos

É possível iniciar a Ferramenta de Serviço a partir da interface da linha de comandos do dispositivo virtual IBM Spectrum Protect Plus e executar a ferramenta em um navegador da web. Em seguida, é possível usar a Ferramenta de Serviço para verificar a conectividade de rede entre o IBM Spectrum Protect Plus e um nó

Procedimento

1. Efetue login no dispositivo virtual IBM Spectrum Protect Plus usando o ID do usuário `serveradmin` e acesse o prompt de comandos. Emita o seguinte comando:

```
# sudo bash
```

2. Abra a porta 9000 no firewall emitindo o seguinte comando:

```
# firewall-cmd --add-port=9000/tcp
```

3. Execute a ferramenta emitindo o seguinte comando:

```
# java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxdd.jar
```

4. Para conectar-se à ferramenta, insira a seguinte URL em um navegador:

```
http:// hostname: 9000
```

em que *hostname* especifica o endereço IP da máquina virtual na qual o aplicativo é implementado.

5. Para especificar o nó para teste, preencha os seguintes campos:

Host

O nome do host ou endereço IP do nó que você deseja testar.

Porta

A porta de conexão a ser testada.

6. Clique em **Salvar**.

7. Para executar a ferramenta, passe o cursor sobre a ferramenta e, em seguida, clique no botão verde **Executar**.

Se uma conexão não puder ser estabelecida, a condição de erro será exibida, junto com possíveis causas e ações.

8. Pare a ferramenta emitindo o seguinte comando na linha de comandos:

```
ctl-c
```

9. Proteja seu ambiente de armazenamento reconfigurando o firewall. Emita os comandos a seguir:

```
# firewall-cmd -- zone=public --remove-port=9000/tcp  
# firewall-cmd---runtime-to-Permanente  
# firewall-cmd -- reload
```

Nota: Se o comando `firewall-cmd` não estiver disponível em seu sistema, edite o firewall manualmente para incluir as portas necessárias e reinicie o firewall usando `iptables`. Para obter mais informações sobre como editar regras de firewall, consulte a seção **Configuração de firewall usando iptables** aqui: https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1adv_firewallportopenexamples.htm.

Executando a Ferramenta de Serviço remotamente

É possível fazer download da Ferramenta de Serviço como um arquivo .jar a partir da interface com o usuário do IBM Spectrum Protect Plus. Em seguida, é possível usar a Ferramenta de Serviço para testar a conectividade remotamente entre o IBM Spectrum Protect Plus e um nó.

Procedimento

1. Na interface com o usuário do IBM Spectrum Protect Plus, clique no menu do usuário e, em seguida, clique em **Fazer download da ferramenta de teste**.
Um arquivo .jar é transferido por download para sua estação de trabalho.
2. Ative a ferramenta a partir de uma interface da linha de comandos. O Java™ é necessário somente no sistema em que a ferramenta será ativada. Os terminais ou sistemas de destino que são testados pela ferramenta não requerem Java.

O comando a seguir ativa a ferramenta em um ambiente Linux:

```
# java -jar -Dserver.port=9000 /<tool path >/ngxdd.jar
```

3. Para conectar-se à ferramenta, insira a seguinte URL em um navegador:

```
http:// hostname: 9000
```

em que *hostname* especifica o endereço IP da máquina virtual na qual o aplicativo é implementado.

4. Para especificar o nó para teste, preencha os seguintes campos:

Host

O nome do host ou endereço IP do nó que você deseja testar.

Porta

A porta de conexão a ser testada.

5. Clique em **Salvar**.

6. Para executar a ferramenta, passe o cursor sobre a ferramenta e, em seguida, clique no botão verde **Executar**.
Se uma conexão não puder ser estabelecida, a condição de erro será exibida, junto com possíveis causas e ações.
7. Pare a ferramenta emitindo o seguinte comando na linha de comandos:

```
ctl-c
```

Incluindo discos virtuais

É possível incluir novos discos virtuais (discos rígidos) em seu dispositivo virtual IBM Spectrum Protect Plus usando o vCenter.

Ao implementar o dispositivo virtual IBM Spectrum Protect Plus, é possível implementar todos os discos virtuais em um banco de dados especificado no momento da implementação. É possível incluir um disco dentro do dispositivo virtual e configurá-lo como um Gerenciador de Volume Lógico (LVM). É possível, então, montar o novo disco como um novo volume ou anexar o novo disco aos volumes existentes no dispositivo virtual.

É possível revisar as partições de disco usando o comando **fdisk -l**. É possível revisar os volumes físicos e os grupos de volumes no dispositivo virtual IBM Spectrum Protect Plus usando os comandos **pvdisplay** e **vgdisplay**.

Incluindo um disco no dispositivo virtual

Use o cliente vCenter para editar as configurações da máquina virtual.

Antes de Iniciar

Para executar comandos, é preciso conectar-se à linha de comandos para o dispositivo virtual IBM Spectrum Protect Plus usando o Shell Seguro (SSH) e efetuar login com o ID do usuário `serveradmin`. A senha inicial padrão é `sppDP758` e é solicitado que mude a senha quando efetuar logon pela primeira vez.

Procedimento

Para incluir um disco em um dispositivo virtual IBM Spectrum Protect Plus, conclua as seguintes etapas a partir do cliente vCenter:

1. No cliente vCenter, conclua as seguintes etapas:
 - a) Na guia **Hardware**, clique em **Incluir**.
 - b) Selecione **Criar um novo disco virtual**.
 - c) Selecione o tamanho do disco necessário. Na seção **Local**, selecione uma das seguintes opções:
 - Para usar o armazenamento de dados atual, selecione **Armazenar com a máquina virtual**.
 - Para especificar um ou mais armazenamentos de dados para o disco virtual, selecione **Especificar um armazenamento de dados ou cluster de armazenamento de dados**. Clique em **Procurar** para selecionar os novos armazenamentos de dados.
 - d) Na guia **Opções avançadas**, deixe os valores padrão.
 - e) Revise e salve suas mudanças.
 - f) Clique na opção **Editar configurações** para a máquina virtual para visualizar o novo disco rígido.
2. Inclua o novo dispositivo SCSI sem reinicializar o dispositivo virtual. No console do dispositivo IBM Spectrum Protect Plus, emita o seguinte comando:

```
echo "-- -" > /sys/class/scsi_host/host#/scan
```

Em que `#` é o número do host mais recente.

Incluindo capacidade de armazenamento de um novo disco para o volume do dispositivo

Depois de incluir um disco no dispositivo virtual, é possível anexar o novo disco aos volumes existentes no dispositivo virtual.

Antes de Iniciar

Para executar comandos, deve-se conectar ao console do dispositivo virtual IBM Spectrum Protect Plus usando SSH e efetuar login com o ID do usuário **serveradmin**. A senha inicial padrão é sppDP758 e é solicitado que mude a senha quando efetuar login pela primeira vez.

Sobre Esta Tarefa

É necessário concluir esta tarefa apenas se desejar incluir a capacidade de armazenamento de um novo disco em um volume do dispositivo existente. Se você incluiu o disco como um novo volume, não será necessário concluir esta tarefa.

Procedimento

Para incluir capacidade de armazenamento de um novo disco no volume do dispositivo, conclua as seguintes etapas a partir do console do dispositivo virtual:

1. Conclua as seguintes etapas para configurar uma partição para o novo disco e configurar a partição para ser do tipo Linux LVM:

- a) Abra o novo disco usando o comando **fdisk**:

```
[ serveradmin@localhost ~ ] # fdisk /dev/sdd
```

O utilitário **fdisk** é iniciado no modo interativo. É exibida uma saída semelhante à seguinte:

```
O dispositivo não contém nenhuma tabela de partição do DOS válida, nem um rótulo de disco Sun, SGI ou OSF
Construindo um novo disco do DOS com o identificador de disco 0xb1b293df.
As mudanças permanecerão somente na memória, até você decidir gravá-las.
Depois disso, é claro, o conteúdo anterior não será recuperável.
Aviso: A sinalização inválida 0x0000 da tabela de partição 4 será corrigida por w(rite)
AVISO: O modo compatível com o DOS foi descontinuado. É altamente recomendado para desativar o modo (comando 'c') e mudar unidades de exibição para setores (comando 'u').
Comando (m para ajuda):
```

- a) Na linha de comandos **fdisk**, insira o subcomando **n** para incluir uma partição.

```
Comando (m para ajuda): n
```

São exibidas as seguintes opções de ação de comando:

```
Comando (m para ajuda): n
Ação de comando
e estendido
partição primária p (1-4)
```

- b) Insira a ação de comando **p** para selecionar a partição primária. É solicitado que forneça um número de partição:

```
Comando (m para ajuda): n
Ação de comando
e estendido
partição primária p (1-4)
Partition number (1-4):
```

- c) No prompt do número de partição, insira o número de partição 1.

```
Partition number (1-4): 1
```

O prompt a seguir é exibido:

```
Primeiro cilindro (1-2610, padrão 1):
```

- d) Não digite nada no prompt do Primeiro cilindro. Pressione a tecla **Enter**. São exibidos a saída e o prompt a seguir:

```
Primeiro cilindro (1-2610, padrão 1):  
Usando o valor padrão 1  
Último cilindro, +cilindros ou +tamanho{K,M,G} (1 a 2610, padrão 2610):
```

- e) Não digite nada no prompt Último cilindro. Pressione a tecla **Enter**. A seguinte saída é exibida:

```
Último cilindro, +cilindros ou +tamanho{K,M,G} (1 a 2610, padrão 2610):  
Usando o valor padrão 2610  
Comando (m para ajuda):
```

- f) Na linha de comandos **fdisk**, insira o subcomando **t** para mudar o ID do sistema de uma partição.

```
Comando (m para ajuda): t
```

É solicitado que forneça um código hexadecimal que identifica o tipo de partição:

```
Partição 1 selecionada  
Código hexadecimal (digite L para códigos de lista):
```

- g) No prompt de Código hexadecimal, insira o código hexadecimal **8e** para especificar o tipo de partição do Linux LVM. A seguinte saída é exibida:

```
Código hexadecimal (digite L para códigos de lista): 8e  
Mudado o tipo de partição do sistema 1 para 8e (Linux LVM)  
Comando (m para ajuda):
```

- h) Na linha de comandos **fdisk**, insira o subcomando **w** para gravar a tabela de partição e para sair do utilitário **fdisk**.

```
Comando (m para ajuda): w
```

A seguinte saída é exibida:

```
Comando (m para ajuda): w (tabela de gravação para disco e saída)  
A tabela de partições foi alterada!  
Chamando ioctl () para reler a tabela de partição.  
Sincronizando os discos.
```

2. Para revisar as mudanças no disco, emita o comando **fdisk -l**.
3. Para revisar a lista atual de Volumes físicos (PV), emita o comando **pvdisplay**.
4. Para criar um novo Volume físico (PV), emita o comando **pvcreate /dev/sdd1**.
5. Para visualizar o novo PV a partir de /dev/sdd1, emita o comando **pvdisplay**.
6. Para revisar o Grupo de volumes (VG), emita o comando **vgdisplay**.
7. Para incluir o Volume físico (PV) no Grupo de volumes (VG) e aumentar o espaço do VG, emita o seguinte comando:

```
vgextend data_vg /dev/sdd1
```

8. Para verificar se `data_vg` foi estendido, e se o espaço livre está disponível para ser usado por volumes lógicos (ou volume `/data`), emita o comando **`vgdisplay`**.
9. Para revisar o volume do Volume lógico (LV) `/data`, emita o comando **`lvdisplay`**. O uso do volume `/data` é exibido.
10. Para incluir o espaço do volume do LV `/data` na capacidade de volume total, emita o comando **`lvextend`**.

Neste exemplo, 20 GB de espaço estão sendo incluídos em um volume de 100 GB.

```
[ serveradmin@localhost ~ ] # lvextend -L120gb -r /dev/data_vg/data
Tamanho do volume lógico data_vg/data mudado de 100,00 GiB para 120,00 GiB.
Dados do volume lógico redimensionados com êxito
resize2fs 1.41.12 (data)
O sistema de arquivos em /dev/mapper/data_vg-data está montado em /data; on-line
redimensionamento requerido
old desc_blocks = 7, new_desc_blocks = 8
Executando um redimensionamento on-line de /dev/mapper/data_vg-data para 31195136
Blocos (4 k).
O sistema de arquivos em /dev/mapper/data_vg-data agora é de 31195136 blocos
de comprimento.
```

Depois de executar o comando precedente, o tamanho do volume `/data` é exibido na saída de comando **`lvdisplay`** como 120 GB:

```
[ serveradmin@localhost ~ ] # lvdisplay
--- Volume lógico ---
LV Path: /dev/data_vg/data
Nome do LV: dados
Nome do VG: data_vg
UUID do LV: [ uuid ]
Acesso de gravação do LV: leitura/gravação
Host de criação do LV, horário localhost.localdomain, [data, hora]
Status do LV: disponível
# open: 1
Tamanho do LV: 120.00 GiB
LE atual: 30208
Segmentos: 2
Alocação herdada
Sector de leitura antecipada: auto
-atualmente configurado como: 256
Dispositivo de bloco: 253: 1
[ serveradmin@localhost ~ ] # df -h
Filesystem                               Size  Used Avail Use% Mounted on
/dev/sda3 14G  2.6G 11G 20% /
tmpfs 16G  0  16G  0% /dev/shm
/dev/sda1 240M  40M 188M 18% /boot
/dev/mapper/data_vg-data
118G  6,4G 104G  6% /data
/dev/mapper/data2_vg-data2
246G  428M 234G  1% /data2
```

Capítulo 12. Gerenciando relatórios e logs

O IBM Spectrum Protect Plus fornece vários relatórios predefinidos que podem ser customizados para atender aos requisitos de relatório. Também é fornecido um log de ações que os usuários concluem no IBM Spectrum Protect Plus.

Tipos de relatório

É possível customizar relatórios predefinidos para monitorar a utilização do armazenamento de backup e outros aspectos do ambiente do sistema.

Os relatórios são baseados nos dados que são coletados pela tarefa de inventário mais recente. É possível gerar relatórios após a conclusão de todas as tarefas de catalogação e as tarefas subsequentes de condensação do banco de dados. É possível executar os seguintes tipos de relatórios:

- Relatórios de Utilização de Armazenamento de Backup
- Relatórios de proteção
- Relatórios do sistema
- Relatórios do Ambiente da Máquina Virtual

Os relatórios incluem elementos interativos, como procurar valores individuais em um relatório, rolagem vertical e classificação de coluna.

Relatórios de Utilização de Armazenamento de Backup

O IBM Spectrum Protect Plus fornece relatórios de utilização de armazenamento de backup que exibem a utilização de armazenamento e o status de seu armazenamento de backup, como servidores vSnap.

Para visualizar relatórios de utilização de armazenamento de backup, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Expanda **Utilização de armazenamento de backup** na área de janela **Relatórios**.

Os seguintes relatórios estão disponíveis:

Utilização de backup da MV

Revise a utilização de seus backups da máquina virtual (VM) no armazenamento de backup, incluindo os dados a seguir:

- O nome de cada VM, seu local e o hypervisor associado.
- A política de SLA que é usada para proteger a VM.
- O local do armazenamento de backup. O armazenamento de backup pode ser o nome do host ou o endereço IP de um disco, o nome de um servidor em nuvem ou o nome do servidor de repositório.
- O tamanho de cada backup de VM.
- O número de pontos de restauração que estão disponíveis para cada VM.

Para máquinas virtuais VMware, para limitar seus resultados para mostrar VMs que têm tags do VMware, selecione uma ou mais tags disponíveis no menu suspenso **Tags**. O valor padrão é **Todos**, que mostra dados para todos os backups de VM.

Relatório de Utilização de Armazenamento vSnap

Revise a utilização de armazenamento de seus servidores vSnap, incluindo o status de disponibilidade, o espaço livre e o espaço usado. O relatório Utilização de armazenamento do vSnap exibe uma visão geral de seus servidores vSnap e uma visualização detalhada das máquinas virtuais e bancos de dados individuais que são protegidos em cada servidor vSnap.

Use as opções de relatório para filtrar servidores vSnap específicos para exibição. Para obter uma visualização detalhada das máquinas virtuais e bancos de dados individuais que são protegidos em

cada servidor vSnap, selecione **Mostrar recursos protegidos pelo armazenamento de vSnap**. Esta área do relatório exibe os nomes das máquinas virtuais, o hypervisor associado, o local e a taxa de compactação/deduplicação do servidor vSnap.

Os valores de capacidade de armazenamento e de uso que são exibidos pelo IBM Spectrum Protect Plus podem variar entre aqueles que aparecem no painel versus aqueles que aparecem no relatório Utilização de armazenamento do vSnap. O painel exibe informações em tempo real, enquanto o relatório reflete dados da última execução da tarefa de inventário. As variações também ocorrem devido a diferentes algoritmos de arredondamento.

Conceitos relacionados

[“Relatar Ações” na página 293](#)

É possível executar, salvar ou planejar relatórios no IBM Spectrum Protect Plus.

[“Tipos de relatório” na página 289](#)

É possível customizar relatórios predefinidos para monitorar a utilização do armazenamento de backup e outros aspectos do ambiente do sistema.

Relatórios de proteção

O IBM Spectrum Protect Plus fornece relatórios que exibem o status de proteção de seus recursos. Ao visualizar os relatórios e executar qualquer ação necessária, é possível ajudar a assegurar que seus dados sejam protegidos por meio de parâmetros de objetivo de ponto de recuperação definidos pelo usuário.

Para visualizar relatórios de proteção, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Expanda **Proteção** na área de janela **Relatórios**.

Os seguintes relatórios estão disponíveis:

Relatório VMs Protegidos e Desprotegidos

Execute o relatório de VMs Protegidas e desprotegidas para visualizar o status de proteção de suas máquinas virtuais. O relatório exibe o número total de máquinas virtuais incluídas no inventário do IBM Spectrum Protect Plus antes do início das tarefas de backup.

Use as opções de relatório para filtrar por tipo de hypervisor e para selecionar hypervisors específicos para exibição.

Para excluir máquinas virtuais desprotegidas no relatório, selecione **Ocultar VMs desprotegidas**.

Para excluir máquinas virtuais que não são submetidas a backup para o armazenamento de backup secundário, selecione **Mostrar apenas as VMs com backups transferidos**.

A **Visualização de resumo** exibe uma visão geral do status de proteção de sua máquina virtual, incluindo o número de máquinas virtuais desprotegidas e protegidas e a capacidade gerenciada das máquinas virtuais protegidas. A capacidade gerenciada é a capacidade utilizada de uma máquina virtual. A **Visualização de detalhes** fornece informações adicionais sobre as máquinas virtuais protegidas e desprotegidas, incluindo nomes e local.

Relatório de Bancos de Dados Protegidos e Desprotegidos

Execute o relatório de Bancos de dados protegidos e desprotegidos para visualizar o status de proteção de seus bancos de dados. O relatório exibe o número total de bancos de dados incluídos no inventário do IBM Spectrum Protect Plus antes do início das tarefas de backup.

Use as opções de relatório para filtrar por tipo de aplicativo, servidor de aplicativos e tipo de servidor de aplicativos para exibição.

Para excluir bancos de dados que são protegidos por meio de tarefas de backup baseadas em hypervisor, selecione **Ocultar bancos de dados protegidos como parte do backup do hypervisor**.

Para excluir bancos de dados desprotegidos no relatório, selecione **Ocultar bancos de dados desprotegidos**.

A **Visualização de resumo** exibe uma visão geral do status de proteção de seu servidor de aplicativos, incluindo o número de bancos de dados desprotegidos e protegidos, bem como a capacidade de front end dos bancos de dados protegidos. A capacidade de front end é a capacidade utilizada de um banco

de dados. A **Visualização de detalhes** fornece informações adicionais sobre os bancos de dados protegidos e desprotegidos, incluindo seus nomes e local

Relatório Histórico de Backup da VM

Execute o relatório de Histórico de backup da VM para revisar o histórico de proteção de máquinas virtuais específicas. Para executar o relatório, pelo menos uma máquina virtual deve ser especificada na opção **VMs**. É possível selecionar vários nomes de máquinas virtuais.

Use as opções de relatório para filtrar por tarefas com falha ou bem-sucedidas e por tempo do último backup. O relatório pode ser melhor filtrado por políticas de acordo de nível de serviço (ANS)

específicas. Na **Visualização de detalhes**, clique no ícone de mais  próximo a uma tarefa associada para visualizar detalhes da tarefa, como a razão pela qual uma tarefa falhou ou o tamanho de um backup bem-sucedido.

Relatório Histórico de Backup de Banco de

Execute o relatório de Histórico de backup de banco de dados para revisar o histórico de proteção de bancos de dados específicos. Para executar o relatório, pelo menos um banco de dados deve ser especificado na opção **Bancos de dados**. É possível selecionar diversos bancos de dados.

Use as opções de relatório para filtrar por tarefas com falha ou bem-sucedidas e por tempo do último backup. O relatório pode ser melhor filtrado por políticas de ANS específicas. Na **Visualização**

detalhada, clique no ícone de sinal de mais  próximo a uma tarefa associada para visualizar outros detalhes da tarefa, como a razão pela qual uma tarefa falhou ou o tamanho de um backup bem-sucedido.

Relatório de Conformidade do RPO de Política do VM S

O relatório Conformidade de RPO da Política de ANS da VM exibe máquinas virtuais em relação a objetivos de ponto de restauração, conforme definido em políticas de ANS. O relatório exibe as seguintes informações:

- Máquinas virtuais em conformidade
- Máquinas virtuais não estão em conformidade
- Máquinas virtuais nas quais a última sessão de tarefa de backup falhou

Use as opções de relatório para filtrar por tipo de hypervisor e para selecionar hypervisors específicos para exibição. O relatório pode ser melhor filtrado por máquinas virtuais que estão em conformidade ou não em conformidade com o RPO definido.

Relatório de Conformidade do RPO de Política do SLA

O relatório Conformidade de RPO da Política de ANS do Banco de Dados exibe bancos de dados em relação a objetivos de ponto de recuperação, conforme definido em políticas de ANS. O relatório exibe as seguintes informações:

- Bases de dados em conformidade
- Bancos de dados não estão em conformidade
- Bancos de dados nos quais a última sessão de tarefa de backup falhou

Use as opções de relatório para filtrar por tipo de aplicativo e para selecionar servidores de aplicativos específicos para exibição. O relatório pode ser melhor filtrado por bancos de dados que estão em conformidade ou não em conformidade com o RPO definido ou por tipo de proteção, incluindo dados que foram submetidos a backup para o vSnap ou usando a replicação.

Conceitos relacionados

“Tipos de relatório” na página 289

É possível customizar relatórios predefinidos para monitorar a utilização do armazenamento de backup e outros aspectos do ambiente do sistema.

Relatórios do sistema

O IBM Spectrum Protect Plus fornece relatórios do sistema que exibem uma visualização detalhada do status de sua configuração, incluindo informações do sistema de armazenamento, tarefas e status da tarefa.

Para visualizar relatórios do sistema, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Expanda **Sistema** na área de janela **Relatórios**.

Os seguintes relatórios estão disponíveis:

Relatório de configuração

Revise a configuração dos servidores de aplicativos, hypervisors e armazenamento de backup que estão disponíveis. Use as opções de relatório para filtrar os tipos de configuração a serem exibidos. O relatório exibe o nome do recurso, tipo de recurso, site associado e o status de conexão SSL.

Relatório de Tarefa

Revise as tarefas disponíveis em sua configuração. Execute o relatório para visualizar tarefas por tipo, sua duração média e sua porcentagem de execução bem-sucedida. Use as opções de relatório para filtrar os tipos de tarefas a serem exibidos e para exibir tarefas que foram executadas com sucesso durante um período de tempo. A **Visualização de resumo** lista tarefas por tipo junto com o número de vezes que uma sessão de tarefa foi executada, concluída ou falhou. Sessões de tarefa listadas como Outras são tarefas que foram interrompidas, parcialmente executadas, estão atualmente em execução, foram ignoradas ou paradas. Na **Visualização detalhada**, clique no ícone de sinal de mais  próximo a uma tarefa associada para visualizar outros detalhes da tarefa, como máquinas virtuais que são protegidas por uma tarefa de backup, o tempo médio de execução e o próximo tempo de execução planejado, se a tarefa estiver planejada.

Relatório de licença

Revise a configuração do ambiente IBM Spectrum Protect Plus em relação a recursos licenciados. As seções e os campos a seguir são exibidos neste relatório:

Proteção da Máquina

O campo **Número total de VMs** exibe o número total de máquinas virtuais protegidas por meio de tarefas de backup do hypervisor, mais o número de máquinas virtuais que hospedam bancos de dados de aplicativo protegidos por meio de tarefas de backup do aplicativo (não tarefas de backup do hypervisor). O campo **Capacidade de front end** exibe o tamanho utilizado dessas máquinas virtuais.

Proteção da Máquina

O campo **Número total de servidores físicos** exibe o número total de servidores de aplicativos físicos que hospedam bancos de dados que são protegidos por tarefas de backup do aplicativo. O campo **Capacidade de front end** exibe o tamanho utilizado desses servidores de aplicativos físicos.

Utilização do armazenamento de backup (vSnap)

O campo **Número total de servidores vSnap** exibe o número de servidores vSnap que estão configurados no IBM Spectrum Protect Plus como um destino de backup. O campo **Capacidade de destino** exibe a capacidade total usada dos servidores vSnap, excluindo os volumes de destino de réplica.

Conceitos relacionados

[“Tipos de relatório” na página 289](#)

É possível customizar relatórios predefinidos para monitorar a utilização do armazenamento de backup e outros aspectos do ambiente do sistema.

relatórios do ambiente de VM

O IBM Spectrum Protect Plus fornece relatórios de ambiente de máquina virtual para exibir a utilização e o status de armazenamento de suas máquinas virtuais e armazenamentos de dados.

Para visualizar relatórios do ambiente de máquina virtual, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Expanda **Ambiente de VM** na área de janela **Relatórios**.

Os seguintes relatórios estão disponíveis:

Relatório de armazenamentos de dados da VM

Revise a utilização de armazenamento de seus armazenamentos de dados, incluindo o espaço livre total, o espaço provisionado e as capacidades. Execute este relatório para visualizar seus armazenamentos de dados, o número de máquinas virtuais nos armazenamentos de dados e a porcentagem de espaço disponível. Use as opções de relatório para filtrar por tipo de hypervisor e para selecionar hypervisors específicos para exibição. O **Filtro da visualização de detalhes** controla os armazenamentos de dados para exibição na **Visualização de detalhes** com base na porcentagem de espaço utilizado. Use o filtro **Mostrar apenas armazenamentos de dados órfãos** para visualizar armazenamentos de dados que não têm nenhuma máquina virtual designada a eles, ou máquinas virtuais que estão em um estado inacessível. A razão para um armazenamento de dados estar em um estado órfão é exibida no campo **Armazenamento de dados** na **Visualização de detalhes**.

Relatório de VM LUNs

Revise a utilização de armazenamento de seus números da unidade lógica (LUNs) da máquina virtual. Execute este relatório para visualizar seus LUNs, armazenamentos de dados, capacidades e fornecedores de armazenamento associados. Use as opções de relatório para filtrar por tipo de hypervisor e para selecionar hypervisors específicos para exibição. Use o filtro **Mostrar apenas armazenamentos de dados órfãos** para visualizar armazenamentos de dados que não têm nenhuma máquina virtual designada a eles, ou máquinas virtuais que estão em um estado inacessível.

Relatório da VM Snapshot Sprawl

Este relatório exibe a idade, o nome e o número de capturas instantâneas que são usadas para proteger os recursos do Hypervisor. Use as opções de relatório para filtrar por tipo de hypervisor e para selecionar hypervisors específicos para exibição. Use o filtro **Horário de criação de captura instantânea** para exibir capturas instantâneas de períodos de tempo específicos.

Relatório VM Sprawl

Revise o status de suas máquinas virtuais, incluindo máquinas virtuais que estão desligadas, ligadas ou suspensas. Execute este relatório para visualizar máquinas virtuais não utilizadas, a data e hora em que elas foram desligadas e os modelos de máquina virtual. Use as opções de relatório para filtrar por tipo de hypervisor e para selecionar hypervisors específicos para exibição. O relatório pode ser melhor filtrado por estado da energia ao longo do tempo, incluindo Dias desde o último desligamento e Dias desde a última suspensão. A seção **Visualização rápida** exibe um gráfico de pizza de espaço utilizado e livre em suas máquinas virtuais com base no estado da energia. Use o filtro **Hypervisor** para exibir máquinas virtuais em todos os hosts ou em um host específico. As informações na **Visualização de detalhes** são categorizadas por estado da energia. É fornecida uma tabela separada para os modelos de máquina virtual.

Relatório de Armazenamento da VM

Revise suas máquinas virtuais e armazenamentos de dados associados neste relatório. Visualize os armazenamentos de dados associados e o espaço provisionado dos armazenamentos de dados. Use as opções de relatório para filtrar por tipo de hypervisor e para selecionar hypervisors específicos para exibição. A **Visualização de detalhes** exibe armazenamentos de dados associados e a quantidade de espaço no armazenamento de dados que está alocado para arquivos de disco virtual.

Conceitos relacionados

[“Tipos de relatório” na página 289](#)

É possível customizar relatórios predefinidos para monitorar a utilização do armazenamento de backup e outros aspectos do ambiente do sistema.

Relatar Ações

É possível executar, salvar ou planejar relatórios no IBM Spectrum Protect Plus.

Executando um relatório

É possível executar relatórios do IBM Spectrum Protect Plus com parâmetros padrão ou executar relatórios customizados com parâmetros customizados.

Procedimento

Para executar um relatório, execute as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Expanda um tipo de relatório e selecione um relatório para ser executado.
3. Execute o relatório com parâmetros customizados ou parâmetros padrão:
 - Para executar o relatório com parâmetros customizados, configure os parâmetros na seção **Opções** e clique em **Executar**. Os parâmetros são exclusivos para cada relatório.
 - Para executar o relatório com parâmetros padrão, clique em **Executar**.

O que Fazer Depois

Revise o relatório na área de janela **Relatórios**.

Conceitos relacionados

[“Gerenciando relatórios e logs” na página 289](#)

O IBM Spectrum Protect Plus fornece vários relatórios predefinidos que podem ser customizados para atender aos requisitos de relatório. Também é fornecido um log de ações que os usuários concluem no IBM Spectrum Protect Plus.

Criando um relatório customizado

É possível modificar relatórios predefinidos com parâmetros customizados no IBM Spectrum Protect Plus e salvar os relatórios customizados.

Procedimento

Para criar um relatório, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Selecione um relatório predefinido.
3. Configure os parâmetros customizados.
4. Defina o relatório para ser executado em uma das seguintes circunstâncias:
 - Executar on demand.
 - Crie um planejamento para executar o relatório conforme definido pelos parâmetros do planejamento.
5. Salve o relatório com um nome customizado.

O que Fazer Depois

Execute o relatório e revise o relatório na área de janela **Relatórios**.

Conceitos relacionados

[“Gerenciando relatórios e logs” na página 289](#)

O IBM Spectrum Protect Plus fornece vários relatórios predefinidos que podem ser customizados para atender aos requisitos de relatório. Também é fornecido um log de ações que os usuários concluem no IBM Spectrum Protect Plus.

Planejando um relatório

É possível planejar relatórios customizados no IBM Spectrum Protect Plus para execução em horários específicos.

Procedimento

Para planejar um relatório, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Selecione um tipo de relatório.
3. Selecione o relatório que você deseja planejar.
4. Edite os parâmetros de relatório na seção **Opções**.
5. Insira valores nos campos **Nome** e **Descrição** para o relatório.
6. Configure os parâmetros para o relatório.
7. Na seção **Planejar relatório**, clique em **Definir planejamento**.
8. Defina um acionador para o relatório.
9. Insira um endereço para receber o relatório planejado no campo de e-mail e, em seguida, clique em **Incluir um destinatário**.
10. Clique em **Salvar**.

O que Fazer Depois

Após a execução do relatório, o destinatário pode revisar o relatório, que é entregue por e-mail.

Conceitos relacionados

[“Gerenciando relatórios e logs” na página 289](#)

O IBM Spectrum Protect Plus fornece vários relatórios predefinidos que podem ser customizados para atender aos requisitos de relatório. Também é fornecido um log de ações que os usuários concluem no IBM Spectrum Protect Plus.

Coletando logs de auditoria para ações

É possível coletar logs de auditoria e procurar ações que são concluídas no IBM Spectrum Protect Plus.

Procedimento

Para coletar logs de auditoria:

1. Na área de janela de navegação, clique em **Relatórios e Logs > Logs de auditoria**.
2. Revise um log de ações que foram concluídas no IBM Spectrum Protect Plus. As informações incluem os usuários que concluíram as ações e as descrições das ações.
3. Para procurar as ações de um usuário específico no IBM Spectrum Protect Plus, insira o nome do usuário no campo de procura do usuário.
4. Opcional: Expanda a seção **Filtros** para filtrar melhor os logs exibidos. Insira descrições de ação específicas e um intervalo de data no qual a ação foi concluída.
5. Clique no ícone procurar .
6. Para fazer download do log de auditoria como um arquivo .csv, clique em **Fazer download** e, em seguida, selecione um local para salvar o arquivo.

Conceitos relacionados

[“Gerenciando contas do usuário” na página 305](#)

Antes de um usuário poder efetuar logon no IBM Spectrum Protect Plus e usar as funções disponíveis, uma conta do usuário deve ser criada no IBM Spectrum Protect Plus.

Capítulo 13. Gerenciando o acesso de

Usando o controle de acesso baseado na função, é possível configurar os recursos e permissões disponíveis para contas do usuário do IBM Spectrum Protect Plus.

É possível customizar o IBM Spectrum Protect Plus para usuários individuais, dando-lhes acesso às características e recursos que eles requerem.

Assim que os recursos estiverem disponíveis para o IBM Spectrum Protect Plus, eles poderão ser incluídos em um grupo de recursos junto com itens de alto nível do IBM Spectrum Protect Plus, como um hypervisor e telas individuais.

As funções são então configuradas para definir as ações que podem ser executadas pelo usuário associado ao grupo de recursos. Essas ações são então associadas a uma ou mais contas do usuário.

Use as seguintes seções da área de janela **Contas** para configurar o acesso baseado em função:

Grupos de Recursos

Um grupo de recursos define os recursos que estão disponíveis para um usuário. Cada recurso incluído no IBM Spectrum Protect Plus pode ser incluído em um grupo de recursos, junto com funções e telas individuais do IBM Spectrum Protect Plus. Ao definir grupos de recursos, é possível otimizar a experiência do usuário. Por exemplo, um grupo de recursos poderia incluir um hypervisor individual, com acesso apenas à funcionalidade de backup e de relatório. Quando o grupo de recursos estiver associado a uma função e a um usuário, o usuário verá apenas as telas que estão associadas ao backup e ao relatório para o hypervisor designado.

Funções

As funções definem as ações que podem ser executadas nos recursos que estão definidos em um grupo de recursos. Enquanto um grupo de recursos define os recursos que serão disponibilizados para uma conta do usuário, uma função configura as permissões para interagir com os recursos definidos no grupo de recursos. Por exemplo, se for criado um grupo de recursos que inclui tarefas de backup e restauração, a função determina como um usuário pode interagir com as tarefas.

As permissões podem ser configuradas para permitir que um usuário crie, visualize e execute as tarefas de backup e restauração que estão definidas em um grupo de recursos, mas não as exclua. De forma semelhante, as permissões podem ser configuradas para criar contas do administrador, permitindo que um usuário crie e edite outras contas, configure sites e recursos e interaja com todos os recursos disponíveis do IBM Spectrum Protect Plus.

Contas de usuário

Uma conta do usuário associa um grupo de recursos a uma função. Para permitir que um usuário efetue login no IBM Spectrum Protect Plus e use suas funções, deve-se primeiro incluir o usuário como um usuário individual (referido como um usuário nativo) ou como parte de um grupo importado de usuários LDAP e, em seguida, designar grupos de recursos e funções à conta do usuário. A conta terá acesso aos recursos e características que estão definidos no grupo de recursos, bem como as permissões para interagir com os recursos e características que estão definidos na função.

Gerenciando grupos de recursos do usuário

Um grupo de recursos define os recursos que são disponibilizados para um usuário. Cada recurso incluído no IBM Spectrum Protect Plus pode ser incluído em um grupo de recursos, junto com funções e telas individuais do IBM Spectrum Protect Plus.

Criando um Grupo de Recursos

Crie um grupo de recursos para definir os recursos que estão disponíveis para um usuário.

Antes de Iniciar

Não é possível designar mais de um aplicativo por máquina como um servidor de aplicativos a um grupo de recursos. Por exemplo, se o SQL e o Exchange ocuparem a mesma máquina e ambos forem registrados no SPP, somente um deles poderá ser incluído como um servidor de aplicativos em um determinado grupo de recursos.

Procedimento

Para criar um grupo de recursos, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Contas > Grupo de recursos**.
2. Clique em **Criar Grupo de Recursos**. A área de janela **Criar Grupo de Recursos** é exibida.
3. Insira um nome para o grupo de recursos.
4. No menu **Quero criar um grupo de recursos**, selecione uma das seguintes opções:

Opção	Ações
Novo(a)	<ol style="list-style-type: none">a. Selecione um tipo de recurso do menu Escolher um tipo de recurso.b. Selecione os subtipos de recursos e, em seguida, clique em Incluir recursos. Os recursos são incluídos na visualização Recursos selecionados.
Do modelo	<ol style="list-style-type: none">a. Selecione um grupo de recursos da lista Qual grupo de recursos você deseja usar como um modelo?. Os recursos do modelo selecionado são incluídos na visualização Recursos selecionados.b. É possível incluir recursos usando a lista Escolher um tipo de recurso e suas listas associadas. <p>Para visualizar os tipos de recursos disponíveis e seu uso, consulte “Tipos de Recursos” na página 298.</p>

Se desejar excluir recursos do grupo, clique no ícone excluir  que está associado a um recurso ou clique em **Excluir todos** para excluir todos os recursos.

5. Quando tiver concluído a inclusão de recursos, clique em **Criar grupo de recursos**.

Resultados

O grupo de recursos é exibido na tabela de grupos de recursos e pode ser associado a contas do usuário novas e existentes.

O que Fazer Depois

Depois de incluir o grupo de recursos, conclua a seguinte ação:

Ação	Como
Crie funções para definir as ações que podem ser executadas pela conta do usuário que está associada ao grupo de recursos. As funções são usadas para definir permissões para interagir com os recursos que estão definidos no grupo de recursos.	Consulte “Criando uma função” na página 302.

Tipos de Recursos

Os tipos de recursos são selecionados quando os grupos de recursos são criados e determinam os recursos que estão disponíveis para um usuário designado a um grupo.

Estão disponíveis os seguintes tipos e subtipos de recursos:

Tipo de Recurso	Subtipo	Descrição
Contas	<ul style="list-style-type: none"> • Função • Usuário • Identidade 	Usado para conceder acesso a funções e usuários por meio da área de janela Contas .
Aplicativo	<ul style="list-style-type: none"> • Db2 • Oracle • Cluster de SQL Independente / Failover • SQL Sempre Ativado 	Usado para conceder acesso para visualização de bancos de dados de aplicativos individuais em um servidor de aplicativos no IBM Spectrum Protect Plus.
Servidor de Aplicativos	<ul style="list-style-type: none"> • Db2 • SQL • Oracle 	Usado para conceder acesso a servidores de aplicativos no IBM Spectrum Protect Plus sem acesso a bancos de dados individuais.
Hypervisor	<ul style="list-style-type: none"> • VMware • Hyper-V 	Usado para conceder acesso a recursos do hypervisor.
Tarefa	Nenhuma	Usado para conceder acesso a tarefas de Inventário, Backup e Restauração. O grupo de recursos de Tarefa é obrigatório para todas as operações de Backup e Restauração, incluindo a designação de Políticas de ANS a recursos.
Relatar	<ul style="list-style-type: none"> • Utilização do Armazenamento de Backup • Proteção • System • Ambiente VE 	Usado para conceder acesso a tipos de relatórios e relatórios individuais.
Tela	Nenhuma	Usado para conceder ou negar acesso a telas na interface do IBM Spectrum Protect Plus. Se determinadas telas não forem incluídas em um grupo de recursos para um usuário, o usuário não será capaz de acessar a funcionalidade fornecida na tela, independentemente das permissões concedidas a ele.
Política do SLA	Nenhuma	Usado para conceder acesso a Políticas de ANS para operações de Backup.

Tipo de Recurso	Subtipo	Descrição
System	Identidade	Usado para conceder acesso às credenciais necessárias para acessar seus recursos. A funcionalidade de identidade está disponível por meio da área de janela Sistema > Identidade .
Configuração do Sistema	Disco	Usado para conceder acesso a servidores de armazenamento de backup vSnap.
Configuração do Sistema	LDAP	Usado para conceder acesso a servidores LDAP para registro do usuário.
Configuração do Sistema	Logs	Usado para conceder acesso para visualização e download de logs de auditoria e do sistema.
Configuração do Sistema	Script	Usado para conceder acesso a pré-scripts e pós-scripts transferidos por upload.
Configuração do Sistema	Servidor de Script	Usado para conceder acesso a servidores de script, nos quais os scripts são executados durante uma tarefa de Backup ou Restauração.
Configuração do Sistema	Site	Usado para conceder acesso a sites, que são designados a servidores de armazenamento de backup vSnap.
Configuração do Sistema	SMTP	Usado para conceder acesso a servidores SMTP para notificações de tarefa.
Configuração do Sistema	Proxy VADP	Usado para conceder acesso a servidores proxy VADP.

Editando um Grupo de Recursos

É possível editar um grupo de recursos para mudar os recursos e características que estão designados ao grupo. As configurações atualizadas do grupo de recursos entram em vigor quando as contas do usuário que estão associadas ao grupo de recursos efetuam login no IBM Spectrum Protect Plus.

Antes de Iniciar

Observe as seguintes considerações antes de editar um grupo de recursos:

- Se você estiver conectado quando as permissões ou os direitos de acesso de sua conta do usuário forem mudados, você deverá sair e conectar-se novamente para que as permissões atualizadas entrem em vigor.
- É possível editar qualquer grupo de recursos que não esteja designado como **Não pode ser modificado**.

Não é possível designar mais de um aplicativo por máquina como um servidor de aplicativos a um grupo de recursos. Por exemplo, se o SQL e o Exchange ocuparem a mesma máquina e ambos forem registrados no SPP, somente um deles poderá ser incluído como um servidor de aplicativos em um determinado grupo de recursos.

Procedimento

Para editar um grupo de recursos, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Grupo de recursos**.
2. Selecione um grupo de recursos e clique no ícone de opções **☰** para o grupo de recursos. Clique em **Modificar recursos**.
3. Revise o nome do grupo de recursos, os recursos ou ambos.
4. Clique em **Atualizar Grupo de Recursos**.

Excluindo um Grupo de Recursos

É possível excluir qualquer grupo de recursos que não esteja designado como **Não pode ser modificado**.

Procedimento

Para excluir um grupo de recursos, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Contas > Grupo de recursos**.
2. Selecione um grupo de recursos e clique no ícone de opções **☰** para o grupo de recursos. Clique em **Excluir grupo de recursos**.
3. Clique em **Sim**.

Gerenciando atribuições

As funções definem as ações que podem ser concluídas para os recursos que são definidos em um grupo de recursos. Enquanto um grupo de recursos define os recursos que estão disponíveis para uma conta, uma função configura as permissões para interagir com os recursos.

Por exemplo, se for criado um grupo de recursos que inclui tarefas de backup e restauração, a função determina como um usuário pode interagir com as tarefas. As permissões podem ser configuradas para permitir que um usuário crie, visualize e execute as tarefas de backup e restauração que estão definidas em um grupo de recursos, mas não as exclua.

De forma semelhante, as permissões podem ser configuradas para criar contas do administrador, permitindo que um usuário crie e edite outras contas, configure sites e recursos e interaja com todos os recursos disponíveis do IBM Spectrum Protect Plus.

A funcionalidade de uma função é dependente de um grupo de recursos configurado corretamente. Ao selecionar uma função predefinida ou configurar uma função customizada, deve-se assegurar que o acesso a operações, telas e recursos necessários do IBM Spectrum Protect Plus esteja alinhado com o uso proposto da função.

As seguintes funções de conta do usuário estão disponíveis:

Admin do Aplicativo

A função de Administrador do aplicativo permite que os usuários conclua as seguintes ações:

- Registrar e modificar recursos do banco de dados de aplicativos que são delegados por um administrador.
- Associe bancos de dados de aplicativos a políticas de ANS designadas.
- Conclua as operações de backup e restauração.
- Execute e planeje relatórios aos quais o usuário tem acesso.

O acesso a recursos deve ser concedido por um administrador por meio da área de janela **Contas > Grupos de recursos**.

Apenas Backup

A função Somente backup permite que os usuários conclua as seguintes ações:

- Executar, editar e monitorar operações de backup

- Visualizar, criar e editar políticas de ANS às quais o usuário tem acesso

O acesso a recursos, incluindo tarefas de backup específicas, deve ser concedido por um administrador clicando em **Contas > Grupos de recursos**.

Restaurar Apenas

A função Somente restauração permite que os usuários concluem as seguintes ações:

- Execute, edite e monitore operações de restauração.
- Visualizar, criar e editar políticas de ANS às quais o usuário tem acesso.

O acesso a recursos, incluindo tarefas de restauração específicas, deve ser concedido por um administrador por meio da área de janela **Contas > Grupos de recursos**.

Autoatendimento

A função de Autoatendimento permite que os usuários monitorem as operações de backup e restauração existentes que são delegadas por um administrador.

O acesso a recursos, incluindo tarefas específicas, deve ser concedido por um administrador por meio da área de janela **Contas > Grupos de recursos**.

SYSADMIN

A função SYSADMIN é a função de administrador. Essa função fornece acesso a todos os recursos e privilégios.

Os usuários com essa função podem incluir usuários e concluir as seguintes ações para todos os usuários diferentes do usuário admin:

- Modificar e excluir contas do usuário
- Alterar senhas do usuário
- Designar funções de usuário

Um administrador também pode acessar o console administrativo selecionando **IBM Spectrum Protect Plus** da lista **Tipo de autenticação** na janela de login do console e inserindo as credenciais de administrador.

No console administrativo, o administrador pode aplicar atualizações de software, reiniciar o dispositivo IBM Spectrum Protect Plus e configurar o fuso horário local.

Para obter informações adicionais sobre como usar o Console Administrativo, consulte [“Efetuando Logon no Console Administrativo”](#) na página 278.

Admin de VM

A função de Administrador da VM permite que um usuário conclua as seguintes ações:

- Registrar e modificar recursos do hypervisor aos quais o usuário tem acesso.
- Associar hypervisors a políticas de SLA.
- Conclua as operações de backup e restauração.
- Execute e planeje relatórios aos quais o usuário tem acesso.

O acesso a recursos deve ser concedido por um administrador por meio da área de janela **Contas > Grupos de recursos**.

Criando uma função

Crie funções para definir as ações que podem ser concluídas pelo usuário de uma conta que está associada a um grupo de recursos. As funções são usadas para definir permissões para interagir com os recursos que estão definidos no grupo de recursos.

Procedimento

Para criar uma função de usuário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Função**.
2. Clique em **Criar Função**. A área de janela **Criar Função** é exibida.

3. Na lista **Quero criar uma função**, selecione uma das seguintes opções:

Opção	Ações
Novo(a)	Selecione as permissões para aplicar à função. Por padrão, nenhuma das permissões é pré-selecionada.
Do modelo	<p>a. Selecione uma função do menu Qual função você quer usar como modelo?. Permissões que estão associadas à função de modelo são selecionadas por padrão.</p> <p>b. Selecione permissões adicionais para aplicar à função e exclua as permissões que não são necessárias.</p> <p>Para visualizar as permissões disponíveis e seu uso, consulte “Tipos de Permissão” na página 303.</p>

4. Insira um nome para a função e, em seguida, clique em **Criar função**.

Resultados

A nova função é exibida na tabela de funções e pode ser aplicada a contas de usuário novas e existentes.

Tipos de Permissão

Os tipos de permissão são selecionados quando as contas do usuário são criadas e determinam as permissões que estão disponíveis para o usuário.

As permissões a seguir estão disponíveis:

Nome	Permissões	Descrição
Aplicativo	Exibir	Usado para visualizar bancos de dados de aplicativos individuais em um servidor de aplicativos no IBM Spectrum Protect Plus.
Servidor de Aplicativos	Register, view, edit, deregister	Usado para interagir com servidores de aplicativos, tais como servidores SQL ou Oracle, sem acesso a bancos de dados individuais.
Certificado	Criar, visualizar, editar, excluir	Usado para interagir com certificados SSL para acessar Servidores em nuvem.
Nuvem	Register, view, edit, deregister	Usado para interagir com Servidores em nuvem que são definidos como armazenamento de backup para transferências.
Hypervisor	Register, view, edit, deregister, options	Usado para interagir com máquinas virtuais do hypervisor, como máquinas virtuais VMware ou Hyper-V.
Identidade e Chaves	Criar, visualizar, editar, excluir	Usado para interagir com as credenciais necessárias para acessar seus recursos. A funcionalidade de identidade está disponível por meio da área de janela Contas > Identidades.

Nome	Permissões	Descrição
LDAP	Register, view, edit, deregister	Usado para interagir com servidores LDAP para registro do usuário.
Log	Exibir	Usado para visualizar logs de Auditoria e do sistema.
Tarefa	Criar, visualizar, editar, executar, excluir	Usado para interagir com tarefas de inventário, de backup e restauração. Nota: Se o usuário tiver permissão para Executar uma tarefa, ele também poderá Suspender, Liberar e Executar ações de restauração customizada para a tarefa
Proxy VADP	Register, view, edit, deregister	Usado para interagir com o VADP
Relatar	Criar, visualizar, editar, excluir	Usado para interagir com relatórios.
Grupo de Recursos	Criar, visualizar, editar, excluir	Usado para interagir com grupos de recursos, que definem os recursos do IBM Spectrum Protect Plus que são disponibilizados para um usuário.
Função	Criar, visualizar, editar, excluir	Usado para interagir com funções, que definem as ações que podem ser executadas nos recursos definidos em um grupo de recursos.
Script	Fazer Upload, visualizar, substituir, excluir	Usado para interagir com pré-scripts e pós-scripts que são incluídos no IBM Spectrum Protect Plus e executados antes ou depois de uma tarefa.
Site	Criar, visualizar, editar, excluir	Usado para interagir com sites, que são designados a servidores de armazenamento de backup vSnap.
SMTP	Register, view, edit, deregister	Usado para interagir com servidores SMTP para notificações de tarefa.
Armazenamento de Backup	Register, view, edit, deregister	Usado para interagir com servidores de armazenamento de backup vSnap.
Política do SLA	Criar, visualizar, editar, excluir	Usado para interagir com Políticas de ANS, que permitem que os usuários criem modelos customizados para tarefas de Backup.

Nome	Permissões	Descrição
Usuário	Criar, visualizar, editar, excluir	Usado para interagir com usuários, que associaram um grupo de recursos a uma função, e fornece acesso à interface com o usuário do IBM Spectrum Protect Plus.

Editando uma função

É possível editar uma função para mudar os recursos e as permissões que estão designados à função. As configurações de função atualizadas entram em vigor quando as contas de usuário que estão associadas à função efetuam login no IBM Spectrum Protect Plus.

Antes de Iniciar

Observe as seguintes considerações antes de editar uma função:

- Se você estiver conectado quando as permissões ou os direitos de acesso de sua conta do usuário forem mudados, você deverá sair e conectar-se novamente para que as permissões atualizadas entrem em vigor.
- É possível editar qualquer função que não esteja designada como **Não pode ser modificada**.

Procedimento

Para editar uma função de usuário, conclua as seguintes etapas

1. Na área de janela de navegação, clique em **Contas > Função**.
2. Selecione uma função e clique no ícone de opções **☰** para a função. Clique em **Modificar Função**.
3. Revise o nome da função, as permissões ou ambos.
4. Clique em **Atualizar Função**.

Excluindo uma função

É possível excluir uma função que não está designada como **Não pode ser modificada**.

Procedimento

Para excluir uma função, execute as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Função**.
2. Selecione uma função e clique no ícone de opções **☰** para a função. Clique em **Excluir função**.
3. Clique em **Sim**.

Gerenciando contas do usuário

Antes de um usuário poder efetuar logon no IBM Spectrum Protect Plus e usar as funções disponíveis, uma conta do usuário deve ser criada no IBM Spectrum Protect Plus.

Criando uma conta do usuário para um usuário individual

Inclua uma conta para um usuário individual no IBM Spectrum Protect Plus. Se estiver atualizando de uma versão do IBM Spectrum Protect Plus que é anterior à 10.1.1, as permissões designadas a usuários na versão anterior devem ser redesignadas no IBM Spectrum Protect Plus.

Antes de Iniciar

Se desejar usar funções e grupos de recursos customizados, crie-os antes de criar um usuário. Consulte [“Criando um Grupo de Recursos”](#) na página 297 e [“Criando uma função”](#) na página 302.

Procedimento

Para criar uma conta para um usuário individual, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Usuário**.
2. Clique em **Incluir Usuário**. A área de janela **Incluir Usuário** é exibida.
3. Clique em **Selecione o tipo de usuário ou grupo que você deseja incluir > Novo usuário individual**.
4. Insira um nome e uma senha para o usuário.
5. Na seção **Designar função**, selecione uma ou mais funções para o usuário.
6. Na seção **Grupos de permissão**, revise as permissões e recursos que estão disponíveis para o usuário e, em seguida, clique em **Continuar**.
7. Na seção **Incluir usuários - Designar recursos**, designe um ou mais grupos de recursos ao usuário e, em seguida, clique em **Incluir recursos**.
Os grupos de recursos são incluídos na seção **Recursos selecionados**.
8. Clique em **Criar usuário**.

Resultados

A conta do usuário é exibida na tabela de usuários. Selecione um usuário da tabela para visualizar funções, permissões e grupos de recursos disponíveis.

Criando uma conta do usuário para um grupo LDAP

Inclua uma conta do usuário para um grupo LDAP no IBM Spectrum Protect Plus.

Antes de Iniciar

Revise os procedimentos a seguir antes de criar uma conta do usuário para um grupo LDAP:

- Registre um provedor LDAP em IBM Spectrum Protect Plus. Consulte [“Incluindo um servidor LDAP”](#) na página 274.
- Se desejar usar funções e grupos de recursos customizados, crie-os antes de criar um usuário. Consulte [“Criando um Grupo de Recursos”](#) na página 297 e [“Criando uma função”](#) na página 302.

Procedimento

Conclua as seguintes etapas para criar uma conta do usuário para um grupo LDAP:

1. Na área de janela de navegação, clique em **Contas > Usuário**.
2. Clique em **Incluir Usuário**. A área de janela **Incluir Usuário** é exibida.
3. Clique em **Selecionar o tipo de usuário ou grupo que você deseja incluir > Grupo LDAP**.
4. Selecione um grupo LDAP.
5. Na seção **Designar função**, selecione uma ou mais funções para o usuário.
6. Na seção **Grupos de permissão**, revise as permissões e recursos que estão disponíveis para o usuário e, em seguida, clique em **Continuar**.
7. Na seção **Incluir usuários - Designar recursos**, designe um ou mais grupos de recursos ao usuário e, em seguida, clique em **Incluir recursos**.
Os grupos de recursos são incluídos na seção **Recursos selecionados**.
8. Clique em **Criar usuário**.

Resultados

A conta do usuário é exibida na tabela de usuários. Selecione um usuário da tabela para visualizar funções, permissões e grupos de recursos disponíveis.

Editando uma Conta do Usuário

É possível editar o nome de usuário, a senha, os grupos de recursos associados e as funções para uma conta do usuário, com exceção de usuários que estão designados à função SUPERUSER. Se um usuário for um membro da função SUPERUSER, será possível mudar apenas a senha para o usuário.

Antes de Iniciar

Se você estiver conectado quando as permissões ou os direitos de acesso de sua conta do usuário forem mudados, você deverá sair e conectar-se novamente para que as permissões atualizadas entrem em vigor.

Procedimento

Conclua as seguintes etapas para editar as credenciais de uma conta do usuário:

1. Na área de janela de navegação, clique em **Contas > Usuário**.
2. Selecione um ou mais usuários. Se você selecionar vários usuários com funções diferentes, será possível modificar apenas seus recursos e não suas funções.
3. Clique no ícone de opções ******* para visualizar as opções disponíveis. As opções que são mostradas dependem do usuário ou usuários selecionados.

Modificar Configurações

Edite o nome de usuário e a senha, as funções associadas e os grupos de recursos.

Modificar recursos

Edite os grupos de recursos associados.

4. Modifique as configurações para o usuário e, em seguida, clique em **Atualizar usuário** ou **Designar recursos**.

Excluindo uma Conta do Usuário

É possível excluir qualquer conta do usuário, com exceção de usuários que estão designados à função SUPERUSER.

Procedimento

Para excluir uma conta do usuário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Usuário**.
2. Selecione um usuário.
3. Clique no ícone de opções ******* e, em seguida, clique em **Excluir usuário**.

Gerenciando identidades

Alguns recursos no IBM Spectrum Protect Plus requerem credenciais para acessar seus recursos. Por exemplo, o IBM Spectrum Protect Plus se conecta a servidores Oracle como o usuário do sistema operacional local que é especificado durante o registro para concluir tarefas, como catalogar, proteção de dados e restauração de dados.

Nomes de usuário e senhas para seus recursos podem ser incluídos e editados por meio da área de janela **Identidade**. Portanto, quando utilizar um recurso no IBM Spectrum Protect Plus que requer credenciais para acessar um recurso, selecione **Usar usuário existente** e selecione uma identidade do menu suspenso.

Incluindo uma Identidade

Inclua uma identidade para fornecer credenciais do usuário.

Procedimento

Para incluir uma identidade, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Identidade**.
2. Clique em **Incluir identidade**.
3. Conclua os campos na área de janela **Propriedades de identidade**:

Nome

Insira um nome significativo para ajudar a identificar a identidade.

Nome de Usuário

Insira o nome do usuário que está associado a um recurso, como um servidor SQL ou Oracle.

Senha

Insira a senha que está associada a um recurso.

4. Clique em **Salvar**.

A identidade é exibida na tabela de identidades e pode ser selecionada quando você está usando um recurso que requer credenciais para acessar um recurso por meio da opção **Usar usuário existente**.

Editando uma Identidade

É possível revisar uma identidade para mudar o nome do usuário e a senha usados para acessar um recurso associado.

Procedimento

Para editar uma identidade, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Identidade**.
2. Clique no ícone editar  que está associado a uma identidade.
A área de janela **Identificar Propriedades** é exibida.
3. Revise o nome da identidade, o nome do usuário e a senha.
4. Clique em **Salvar**.

A identidade revisada é exibida na tabela de identidades e pode ser selecionada ao utilizar um recurso que requer credenciais para acessar um recurso por meio da opção **Usar usuário existente**.

Excluindo uma Identidade

É possível excluir uma identidade quando ela se tornar obsoleta. Se uma identidade estiver associada a um servidor de aplicativos registrado, ela deverá ser removida do servidor de aplicativos antes de poder ser excluída. Para remover a associação, navegue para a página **Backup > Gerenciar servidores de aplicativos** associada ao tipo de servidor de aplicativos, em seguida, edite as configurações do servidor de aplicativos.

Procedimento

Para excluir uma identidade, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Contas > Identidade**.
2. Clique no ícone excluir  que está associado a uma identidade.
3. Clique em **Sim** para excluir a identidade.

Capítulo 14. Licenciamento

A auditoria de licença no IBM Spectrum Protect Plus é ativada por padrão para determinar se o uso atual está dentro dos níveis de autorização de licença e evitar potenciais violações de licença.

O IBM Spectrum Protect Plus gera logs de auditoria de autorização como arquivos do IBM® Software License Metric Tag (.slmtag). O IBM® License Metric Tool (ILMT) é então usado para converter o arquivo e gerar Relatórios de consumo de licença. Use as informações nesta seção para interpretar os arquivos .slmtag.

Tags do Software License Metric (SLM)

O IBM Spectrum Protect Plus gera logs de auditoria de autorização como arquivos do IBM® Software License Metric Tag (.slmtag). O IBM® License Metric Tool (ILMT) é então usado para converter o arquivo e gerar Relatórios de consumo de licença. Use as informações fornecidas para interpretar os arquivos .slmtag.

Os arquivos .slmtag podem armazenar informações até um tamanho máximo de arquivo de 1 MB, após o qual o arquivo é arquivado e um novo arquivo de log é criado. É mantido um máximo de 10 arquivos de log.

Requisitos de Upgrade: Se estiver atualizando para o IBM Spectrum Protect Plus 10.1.3 de uma liberação anterior, deve-se executar a tarefa de manutenção para gerar os arquivos .slmtag. Para upgrades futuros, deve-se executar a tarefa de manutenção para atualizar arquivos .slmtag existentes.

Formato de log

Os arquivos .slmtag são armazenados em formato XML, com novos registros de métrica anexados ao final do arquivo.

A seguir está um arquivo .slmtag de amostra:

```
< SchemaVersion> 2.1.1 < /SchemaVersion>
< SoftwareIdentity>
  <SoftwareIdentity name>"IBM Spectrum Protect Plus"</Name>
  < InstanceId> /opt/virgo < /InstanceId>
< /SoftwareIdentity>
< Metric logTime = "2018-11-05T16:05:09 + 00:00">
  < Type> HYPERVISOR_SERVER_COUNT < /Type>
  < SubType> HYPERVISOR_SERVER_COUNT < /SubType>
  <Value>0</Value>
  < Period>
    < StartTime> 2018-11-05T16:05:09 + 00:00 < /StartTime>
    < EndTime> 2018-11-05T16:05:09 + 00:00 < /EndTime>
  < /Period>
< /Metric>
< Metric logTime = "2018-11-05T16:05:09 + 00:00">
  < Type> APPLICATION_INSTANCE_COUNT < /Type>
  < SubType> APPLICATION_INSTANCE_COUNT < /SubType>
  <Value>0</Value>
  < Period>
    < StartTime> 2018-11-05T16:05:09 + 00:00 < /StartTime>
    < EndTime> 2018-11-05T16:05:09 + 00:00 < /EndTime>
  < /Period>
< /Metric>
```

em que o elemento Value exibe o número de hosts em todos os grupos de recursos com pacotes implementados para um grupo de instâncias, no horário especificado no elemento EndTime.

O arquivo cresce ao longo do tempo e pode ser editado para remover elementos de métrica mais antigos. Certifique-se de manter os elementos por tempo suficiente para varredura de ILMT; a frequência de

varredura é determinada pelo administrador do ILMT, mas geralmente, deve ser suficiente manter os elementos por um mês.

Local do Log

O arquivo `.slmtag` está localizado no diretório `/data/slmtag`.

Conceitos relacionados

[“Tipos de Tarefa” na página 251](#)

As tarefas são usadas para executar operações de backup, restauração, manutenção e inventário no IBM Spectrum Protect Plus.

Tarefas relacionadas

[“Iniciando Tarefas” na página 252](#)

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Integração com o IBM License Metric Tool (ILMT)

Use o IBM License Metric Tool (ILMT) para ajudar a determinar se seu ambiente do sistema está em conformidade com os requisitos de licenciamento.

O ILMT fornece recursos úteis para gerenciar ambientes virtualizados e medir a utilização da licença. O ILMT descobre o software que está instalado em sua infraestrutura, ajuda a analisar os dados de consumo e permite gerar relatórios de auditoria. Cada relatório fornece diferentes informações sobre sua infraestrutura, por exemplo os grupos de computadores, as instalações de software e o conteúdo de seu catálogo do software.

Por padrão, cada relatório de auditoria do ILMT apresenta dados dos 90 dias anteriores. É possível customizar o tipo e a quantidade de informações exibidas em um relatório usando filtros e salvar suas configurações pessoais para uso futuro. Também é possível exportar os relatórios para o formato `.csv` ou `.pdf` e planejar e-mails de relatório para que os destinatários especificados sejam notificados quando ocorrerem eventos importantes.

Para obter mais informações, consulte a documentação do produto [IBM License Metric Tool](#).

Capítulo 15. Detecção de problemas

Procedimentos de resolução de problemas estão disponíveis para diagnóstico e resolução de problemas.

Para obter uma lista de problemas conhecidos e limitações para cada liberação do IBM Spectrum Protect Plus, consulte [nota técnica 2014120](#).

Coletando Arquivos de Log para Resolução de Problemas

Para resolver problemas do aplicativo IBM Spectrum Protect Plus, é possível fazer download de um archive de arquivos de log que são gerados pelo IBM Spectrum Protect Plus.

Procedimento

Para coletar arquivos de log para resolução de problemas, conclua as seguintes etapas:

1. Clique no menu do usuário e, em seguida, clique em **Fazer download de logs do sistema**.
O processo de download pode levar algum tempo para ser concluído.
2. Abra ou salve o arquivo zip do log de arquivo, que contém arquivos de log individuais para diferentes componentes do IBM Spectrum Protect Plus.

Para obter informações sobre arquivos de log, consulte as seções de proteção de aplicativos ou de proteção de backup de hypervisores.

O que Fazer Depois

Para resolver problemas, conclua as seguintes etapas:

1. Analise os arquivos de log e execute ações apropriadas para resolver o problema.
2. Se não for possível resolver o problema, envie os arquivos de log para o Suporte de software IBM para obter assistência.

Capítulo 16. Mensagens do produto

Os componentes do IBM Spectrum Protect Plus enviam mensagens com prefixos que ajudam a identificar de qual componente eles são provenientes. Use a opção de procura para localizar uma mensagem específica usando seu identificador exclusivo.

As mensagens consistem nos seguintes elementos:

- Um prefixo de cinco letras.
- Um número para identificar a mensagem.
- O texto da mensagem exibido na tela e gravado para os logs de mensagens.

Dica: Use o recurso de procura de seu navegador usando Ctrl + F para localizar o código de mensagem que você está procurando.

O exemplo a seguir contém o prefixo do agente do Db2. Ao clicar em Mais, são mostrados detalhes adicionais que explicam o motivo da mensagem.

```
Advertência
Apr 16, 2019
9:14:37 AM
GTGGH0098
[myserver1.myplace.irl.ibm.com]
Database AC7 will not be backed up as it is ineligible for the backup operation. More
```

Prefixos de mensagem do IBM Spectrum Protect Plus

As mensagens possuem prefixos diferentes para ajudar a identificar o componente que emite a mensagem.

A tabela a seguir identifica o prefixo que está associado a cada componente.

Prefixo	Componente
CTGGA	IBM Spectrum Protect Plus
CTGGB	IBM Spectrum Protect Plus servidor vSnap
CTGGC	IBM Spectrum Protect Plus VDAP (VMware e Hyper-V)
CTGGD	IBM Spectrum Protect Plus Nuvem e S3
CTGGE	IBM Spectrum Protect Plus for Microsoft SQL Server
CTGGF	IBM Spectrum Protect Plus para Oracle
CTGGG	IBM Spectrum Protect Plus for Microsoft Exchange Server
CTGGH	IBM Spectrum Protect Plus para IBM Db2
CTGGI	IBM Spectrum Protect Plus para MongoDB

Para obter uma lista de todas as mensagens, consulte o IBM Knowledge Centre [aqui](#).

Apêndice A. Diretrizes de Procura

Use filtros para procurar uma entidade, como um arquivo ou um ponto de restauração.

É possível inserir uma sequência de caracteres para localizar objetos com um nome que corresponda exatamente à sequência de caracteres. Por exemplo, procurar o termo `string.txt` retorna a correspondência exata, `string.txt`.

As entradas de procura de expressão regular também são suportadas. Para obter mais informações, consulte [Pesquisar Texto com Expressões Regulares](#).

Também é possível incluir os seguintes caracteres especiais na procura. Deve-se usar um caractere de escape barra invertida (`\`) antes de qualquer um dos caracteres especiais:

```
+ - & | ! ( ) { } [ ] ^ " ~ * ? : \
```

Por exemplo, para procurar o arquivo `string[2].txt`, insira `string\[2\].txt`.

Procurando com Caracteres Curinga

É possível posicionar os curingas no início, no meio ou no final de uma sequência e combiná-los em uma sequência.

Corresponder uma sequência de caracteres com um asterisco

Os exemplos a seguir mostram o texto da procura com um asterisco:

- `string*` procura termos como `string`, `strings` ou `stringency`
- `str*ing` procura termos como `string`, `straying` ou `straightening`
- `*string` procura termos como `string` ou `shoestring`

É possível usar vários curingas asteriscos em uma única sequência de texto, mas vários curingas podem deixar uma grande procura consideravelmente lenta.

Corresponder um único caractere com um ponto de interrogação:

Os exemplos a seguir mostram o texto da procura com um ponto de interrogação:

- `string?` procura termos como `strings`, `stringy` ou `string1`
- `st??ring` procura termos como `starring` ou `steering`
- `???string` procura termos como `hamstring` ou `bowstring`

Apêndice B. 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](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/), para assegurar conformidade com o [US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) (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](http://www.w3.org/TR/WCAG20/) (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](http://www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility) (www.ibm.com/support/knowledgecenter/about/releasenotes.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).

Avisos

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 ter uma cópia do produto ou da versão de produto nesse idioma para acessá-lo.

A IBM pode não oferecer os produtos, serviços ou recursos discutidos neste documento em outros países. Consulte o representante local da IBM para obter informações sobre os produtos e serviços atualmente disponíveis na sua área. Qualquer referência a um produto, programa ou serviço IBM não se destina a declarar nem deixar implícito que apenas aquele produto, programa ou serviço IBM pode ser usado. Qualquer produto, programa ou serviço funcionalmente equivalente que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser usado em substituição. No entanto, é responsabilidade do usuário avaliar e verificar a operação de qualquer produto, programa ou serviço não IBM.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas aos 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.

Essas informações podem 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 aperfeiçoar e/ou mudar produtos e/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 nesta publicação e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do IBM Customer Agreement, do Contrato de Licença do Programa Internacional IBM ou qualquer contrato equivalente entre nós.

Os dados de desempenho discutidos aqui são apresentados como derivados sob as condições de operação específicas. Os resultados reais podem variar.

Informações com relação a produtos não IBM foram obtidas dos fornecedores desses produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou esses 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 direcionadas a seus fornecedores.

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, uso, 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 nenhum tipo. A IBM não deve ser responsabilizado por quaisquer danos oriundos do 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. _digite o ano ou anos_.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas comerciais ou marcas registradas da International Business Machines Corp., registradas em várias jurisdições no mundo todo. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atual das marcas comerciais da IBM está disponível na Web em "Copyright and trademark information" em 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, outros países ou ambos.

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou registradas da Oracle e/ou suas afiliadas.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

VMware, VMware vCenter Server e VMware vSphere são marcas registradas ou marcas comerciais da VMware, Inc. ou de suas subsidiárias nos Estados Unidos e/ou outras jurisdições.

Termos e condições para a documentação do produto

Permissões para o uso dessas publicações são concedidas sujeitas aos seguintes termos e condições.

Aplicabilidade

Além disso, esses termos e condições complementam quaisquer termos de uso para o website da IBM.

Uso pessoal

Você pode reproduzir estas publicações para uso pessoal não comercial, desde que todos os avisos do proprietário sejam preservados. Você não pode distribuir, exibir ou criar trabalho derivado destas publicações, ou de qualquer parte delas, sem o consentimento expresso da IBM.

Uso comercial

Você pode reproduzir, distribuir e exibir estas publicações unicamente dentro da sua empresa, desde que todos os avisos do proprietário sejam preservados. Você não pode criar 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 conforme explicitamente concedido nesta permissão, nenhuma outra permissão, licença ou direito é concedido, sejam explícitos ou implícitos, para as publicações ou quaisquer informações, dados, software ou outra propriedade intelectual contida neste documento.

A IBM reserva-se o direito de cancelar as permissões concedidas aqui sempre que, a seu critério, achar que o uso das publicações é prejudicial aos seus interesses ou, conforme determinado pela IBM, as instruções acima não estiverem sendo corretamente seguidas.

Você não pode fazer download, exportar ou reexportar estas informações, exceto em conformidade total com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentos de exportação dos Estados Unidos.

A IBM NÃO FORNECE GARANTIA QUANTO AO CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE ENCONTRAM", SEM GARANTIA DE NENHUM TIPO, SEJA EXPLÍCITA OU IMPLÍCITA, INCLUINDO, ENTRE OUTRAS, GARANTIAS IMPLÍCITAS DE CAPACIDADE DE COMERCIALIZAÇÃO, NÃO INFRAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

Considerações sobre política de privacidade

Os produtos de Software IBM, incluindo soluções de software como serviço (“Ofertas de Software”) podem usar cookies ou outras tecnologias para coletar informações de uso do produto, ajudar a melhorar a experiência do usuário final, customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação identificável pessoalmente é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem permitir a coleta de informações identificáveis pessoalmente. Se as Ofertas de Software usarem cookies para coletar informações identificáveis pessoalmente, informações específicas sobre o uso de cookies desta oferta serão estabelecidas abaixo.

Esta Oferta de Software não usa cookies ou outras tecnologias para coletar informações identificáveis pessoalmente.

Se as configurações implementadas para esta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações identificáveis pessoalmente dos usuários finais por meio de cookies e outras tecnologias, deve-se consultar seu próprio conselho jurídico sobre as leis aplicáveis a tal coleta de dados, incluindo os requisitos para 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](#).

Índice Remissivo

A

acesso de usuário [5](#), [297](#)
acordo de nível de serviço, *Veja* Políticas de SLA
ambientes virtuais [265](#)
Arquivamento de log
 Db2 [150](#)
arquivos
 pesquisando por [315](#)
 restauração [133](#)
atualizações de disponibilidade antecipada, obtendo e aplicando [88](#)
atualizações off-line [83](#)
atualizações online [83](#)

B

backup
 tarefas
 on demand [254](#)
Backup de log do Db2 [150](#)

C

certificado
 excluindo [270](#)
 incluindo [269](#)
Certificado SSL, fazendo upload
 a partir da linha de [281](#)
 a partir do console administrativo [280](#)
chave
 excluindo [269](#), [271](#)
 incluindo [269](#), [270](#)
chaves [268](#)
Configurando o Db2
 Opções de SLA [148](#)
Console Administrativo, efetuando logon no [278](#)
Controle de Acesso
 MongoDB [197](#)
criação
 funções [302](#)
 grupos de recursos [297](#)
 Políticas de SLA [89](#)
 Proxies VADP [108](#)
 relatórios [294](#)
 usuários
 grupo LDAP [306](#)
 individual [305](#)

D

data protection [265](#)
Db2
 requisitos do sistema [31](#)
Detectando
 Db2 [142](#)

Dispositivo virtual
 atualizando o [83](#)
Dispositivo Virtual
 acesso
 no Hyper-V [282](#)
 no VMware [281](#)
 incluindo capacidade de armazenamento [285](#)
 incluindo um disco para [284](#)
 instalando
 no Hyper-V [48](#)
 no VMware [46](#)
Dispositivo virtual vCenter baseado no Linux, fazendo backup [107](#)

E

editando
 configurações [276](#)
 funções [305](#)
 grupos de recursos [300](#)
 identidades [308](#)
 Políticas de SLA [93](#)
 Servidor LDAP [276](#)
 Servidor SMTP [276](#)
 sites [272](#)
 usuários [307](#)
efix [88](#)
Exchange Server
 requisitos do sistema [28](#)
excluindo
 demo de SLA [93](#)
 funções [305](#)
 grupos de recursos [301](#)
 identidades [308](#)
 Políticas de SLA [93](#)
 Servidor LDAP [277](#)
 Servidor SMTP [277](#)
 sites [273](#)
 usuários [307](#)

F

Fazendo backup
 Db2 [144](#)
firewalls [51](#)
funções
 criação [302](#)
 editando [305](#)
 excluindo [305](#)
 tipos de permissão [303](#)
fuso horário, configuração [279](#)

G

grupos de recursos
 criação [297](#)

grupos de recursos (*continuação*)

editando [300](#)
excluindo [301](#)
tipos de [298](#)

H

Hyper-V

Dispositivo Virtual
 acesso [282](#)
 incluindo [121](#)
 instalando no dispositivo virtual [48](#)
servidores
 ativando o WinRM [123](#)
 detectando recursos para [123](#)
 testando a conexão com [123](#)
 tarefa de backup, criando [124](#)
 tarefa de restauração, criando [127](#)

I

IBM Knowledge Center [vii](#)

identidades

 editando [308](#)
 excluindo [308](#)
 incluindo [307](#)

incapacidade [317](#)

incluindo

 discos virtuais para uma máquina virtual vCenter [284](#)
 identidades [307](#)
 Instâncias do vCenter Server [95](#)
 Servidor LDAP [274](#)
 Servidor SMTP [275](#)
 servidores de aplicativos Oracle [235](#)
 Servidores de aplicativos SQL Server [223](#)
 servidores Hyper-V [121](#)
 servidores vSnap [56](#)
 sites [119](#), [271](#)

Incluindo Db2 [141](#)

Incluindo o MongoDB [199](#)

Incluir Partições Db2 [141](#)

iniciação rápida [69](#)

iniciando

 IBM Spectrum Protect Plus [71](#)
 tarefas
 no planejamento [89](#)
 on demand [252](#)

instalando

 Dispositivo Virtual
 no Hyper-V [48](#)
 no VMware [46](#)
 pacotes de download, obtendo [45](#)
 servidores vSnap
 ambiente de VMware [54](#)
 ambiente do Hyper-V [55](#)
 ambiente físico [53](#)

K

Knowledge Center [vii](#)

L

LDAP

 grupo, criando uma conta do usuário para [306](#)
 server

 configurações, editando [276](#)
 excluindo [277](#)
 incluindo [274](#)

Localizando o Db2 [142](#)

logs

 auditoria
 fazendo download [295](#)
 visualizando [295](#)
 system
 fazendo download [311](#)
 visualizando [311](#)

M

mensagem

 prefixos [313](#)

mensagens [313](#)

MongoDB

 requisitos do sistema [34](#)

N

Novo no IBM Spectrum Protect Plus Versão Versão 10.1.4 [ix](#)

O

Opções de SLA

 Db2 [148](#)

Oracle

 bancos de dados multiencadeados [235](#)
 requisitos do sistema [37](#)
 servidores de aplicativos
 detectando recursos para [236](#)
 incluindo [235](#)
 testando a conexão com [237](#)
 tarefa de backup, criando [237](#)
 tarefa de restauração, criando [240](#)

P

Planejamento [251](#)

Planejar tarefas

 Backup [146](#), [165](#), [205](#)

 políticas de backup, *Veja* Políticas de SLA

 Políticas de SLA

 editando [93](#)
 excluindo [93](#)
 incluindo [89](#)

 pontos de restauração, excluindo [249](#)

 pontos de restauração, gerenciando [248](#)

 pré-requisito

 Db2 [137](#)
 MongoDB [197](#)

 Pré-requisitos

 MongoDB [197](#)

 preferências

 global
 gerenciando [277](#)

- preferências globais
 - gerenciando [277](#)
- Programa beta
 - vantagens [xi](#)
 - visão geral [geral xi](#)
- programa do usuário patrocinador
 - vantagens [xi](#)
 - visão geral [geral xi](#)
- provedor do servidor de repositório
 - editando [268](#)
 - excluindo [268](#)
- provedor em nuvem
 - editando [261](#)
 - excluindo [261](#)
- Proxies VADP
 - atualizando o [87](#)
 - criação [108](#)
 - opções, configurando [110](#)
 - removendo a instalação [111](#)
- publicações [vii](#)

R

- RBAC
 - MongoDB [197](#)
- recursos de acessibilidade [317](#)
- rede
 - testando [282](#), [283](#)
- rede fenced, criando [118](#)
- reexecutar
 - tarefas
 - on demand [253](#)
- relatórios
 - customizado, criando [294](#)
 - executando
 - no planejamento [294](#)
 - on demand [294](#)
 - tipos de
 - ambiente de VM [292](#)
 - proteção [290](#)
 - system [291](#)
 - utilização de armazenamento de backup [289](#)
- requisitos do sistema
 - componentes [11](#)
 - Db2 [31](#)
 - Exchange Server [28](#)
 - hypervisores [23](#)
 - índice de arquivo e restauração [24](#)
 - MongoDB [34](#)
 - Oracle [37](#)
 - SQL Server [41](#)
- Restaurando
 - Db2 [151](#), [155](#), [158](#)
- Restaurando o Db2
 - Instância alternativa [158](#)
 - Instância original [155](#)
- restaurar tarefas
 - criação
 - Hyper-V [127](#)
 - IBM Spectrum Protect Plus [247](#)
 - Oracle [240](#)
 - SQL Server [228](#)
 - VMware [111](#)
 - executando

- restaurar tarefas (*continuação*)
 - executando (*continuação*)
 - Hyper-V [127](#)
 - Oracle [240](#)
 - SQL Server [228](#)
 - VMware [111](#)

S

- scripts para operações de backup e restauração
 - fazendo upload [255](#)
- servidor de aplicativos
 - Db2 [137](#)
- Servidor de aplicativos MongoDB [196](#)
- Servidor de proteção de espectro IBM
 - incluindo um servidor de repositório [267](#)
- servidor em nuvem
 - incluindo um recurso de nuvem amazon s3 [257](#)
 - incluindo um recurso de nuvem Microsoft azure [260](#)
 - incluindo um recurso do IBM Cloud Object Storage [259](#)
- servidor vSnap
 - administrando
 - administração de armazenamento [63](#)
 - administração de rede [66](#)
 - conjuntos de armazenamentos, expandindo [60](#)
 - editando [58](#)
 - excluindo [58](#)
 - inicializando
 - avançado [59](#)
 - simple [58](#)
 - mudar rendimento [61](#)
 - opções de armazenamento, gerenciando [59](#)
 - parceria de replicação, estabelecendo [60](#)
- servidores vSnap
 - incluindo [56](#)
 - instalando
 - ambiente de VMware [54](#)
 - ambiente do Hyper-V [55](#)
 - ambiente físico [53](#)
 - removendo a instalação [66](#)
- sites
 - editando [272](#)
 - excluindo [273](#)
 - incluindo [119](#), [271](#)
 - regulador [271](#), [272](#)
- SLA [146](#), [165](#), [205](#)
- SMTP
 - server
 - configurações, editando [276](#)
 - excluindo [277](#)
 - incluindo [275](#)
- SQL Server
 - requisitos do sistema [41](#)
 - requisitos para proteção de dados [222](#)
 - servidores de aplicativos
 - detectando recursos para [224](#)
 - incluindo [223](#)
 - testando a conexão com [225](#)
 - tarefa de backup, criando [225](#)
 - tarefa de restauração, criando [228](#)

T

- t_object_agent_client_sppIBM Spectrum Protect Plus [265](#)
- tarefas
 - cancelando [253](#)
 - fazendo backup de um único recurso [254](#)
 - iniciando
 - no planejamento [89](#)
 - on demand [252](#)
 - liberando [253](#)
 - nomes de [251](#)
 - pausando [253](#)
 - reexecutar [253](#)
 - tipos de [251](#)
- tarefas de backup
 - ad hoc
 - on demand [254](#)
 - criação
 - Hyper-V [124](#)
 - IBM Spectrum Protect Plus [247](#)
 - Oracle [237](#)
 - SQL Server [225](#)
 - VMware [103](#)
 - excluindo VMDKs de [107](#)
 - iniciando
 - no planejamento [89](#)
 - on demand [252](#)
 - reexecutar
 - on demand [253](#)
- Tarefas e Operações [251](#)
- teclado [317](#)
- Testando a conexão
 - Db2 [143](#)
- Transferência
 - Servidor IBM Spectrum Protect [262](#)

U

- usuários
 - editando [307](#)
 - excluindo [307](#)
 - funções
 - criação [302](#)
 - editando [305](#)
 - excluindo [305](#)
 - tipos de permissão [303](#)
 - grupo LDAP, criando [306](#)
 - grupo de recursos
 - criação [297](#)
 - editando [300](#)
 - excluindo [301](#)
 - tipos de [298](#)
 - indivíduo, criando [305](#)

V

- VMware
 - Dispositivo Virtual
 - acesso [281](#)
 - instalando no dispositivo virtual [46](#)
 - Instâncias do vCenter Server
 - incluindo [95](#)
 - privilégios da máquina virtual, necessários [96](#)

VMware (continuação)

- tarefa de backup, criando [103](#)
- tarefa de backup, excluindo VMDKs da política de ANS [107](#)
- tarefa de restauração
 - criando uma rede fenced [118](#)
- tarefa de restauração, criando [111](#)
- vCenter Server, detectando recursos [102](#)
- vCenter Server, testando a conexão com [102](#)
- vSnap
 - atualizando o [86](#)

W

- WinRM, ativando para conexão com servidores Hyper-V [123](#)



Printed in USA