

IBM Spectrum Protect Plus
Versão 10.1.6

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 555](#).

Terceira edição (26 de junho de 2020)

Esta edição se aplica à versão 10, liberação 1, modificação 6 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, 2020.

Índice

Sobre esta publicação.....	ix
Quem Deve Ler essa Publicação.....	ix
Publicações	ix
O Que Há de Novo em Versão 10.1.6.....	xi
Envolvendo-se no desenvolvimento do produto.....	xiii
Programa do usuário patrocinador.....	xiii
Programa beta.....	xiii
Capítulo 1. Visão geral do produto.....	1
Storyboard de implementação.....	1
Componentes do Produto.....	6
Painel do Produto.....	8
Alertas.....	10
Controle de Acesso Baseado na Função.....	10
Replicar dados de armazenamento de backup.....	11
Copiar capturas instantâneas para armazenamento de backup secundário.....	11
IBM Spectrum Protect Plus no IBM Cloud.....	14
IBM Spectrum Protect Plus on AWS.....	15
Integração com o IBM Spectrum Protect.....	16
Incluindo o IBM Spectrum Protect Plus no Centro de operações.....	17
Inserindo a URL do Operations Center.....	19
Acessando o Operations Center.....	20
Capítulo 2. Instalando o IBM Spectrum Protect Plus.....	23
Roteiro de implementação do produto.....	23
Requisitos de Sistema	23
Requisitos do Componente	23
Requisitos do hypervisor e da instância da nuvem	40
Requisitos de Indexação de Arquivo e Restauração.....	43
Requisitos do Sistema de arquivos.....	50
Requisitos do Suporte de Backup de Kubernetes.....	54
Requisitos do Db2.....	60
Requisitos do Microsoft Exchange Server.....	66
Requisitos do MongoDB.....	72
Requisitos do Office 365.....	78
Requisitos do Oracle.....	82
Requisitos do Microsoft SQL Server.....	90
Obtendo o pacote de instalação do IBM Spectrum Protect Plus.....	98
Instalando o IBM Spectrum Protect Plus como um dispositivo virtual VMware.....	99
Instalando o IBM Spectrum Protect Plus como um dispositivo virtual Hyper-V.....	101
Designando um endereço IP estático.....	103
Fazendo Upload da Chave do Produto.....	104
Editando portas de firewall.....	104
Instalando utilitários de inicializadores iSCSI.....	106
Capítulo 3. Instalando servidores vSnap.....	109
Instalando um servidor vSnap.....	109
Instalando um servidor vSnap físico.....	109

Instalando um servidor vSnap virtual em um ambiente VMware.....	110
Instalando um servidor vSnap virtual em um ambiente Hyper-V.....	112
Desinstalando um servidor vSnap.....	113
Capítulo 4. Gerenciando servidores vSnap.....	115
Registrando um servidor vSnap.....	115
Editando Configurações para um Servidor vSnap.....	116
Configurando opções de armazenamento de backup.....	118
Como excluir e recriar um conjunto de armazenamentos do vSnap?.....	124
Inicializando o servidor vSnap.....	126
Concluindo uma inicialização simples.....	127
Concluindo uma Inicialização Avançada.....	127
Expandindo um conjunto de armazenamentos vSnap.....	128
Mudando a taxa de rendimento.....	128
Substituindo um servidor vSnap com falha.....	129
Referência de administração do servidor vSnap	129
Gerenciamento do Usuário.....	130
Gerenciamento de armazenamento.....	131
Gerenciamento de rede.....	134
Cabeçalhos e ferramentas do kernel.....	135
Resolução de problemas de servidores vSnap.....	136
Sincronizando a senha vSnap.....	136
Por que o servidor vSnap ainda está off-line?.....	136
Posso reparar um servidor vSnap com falha no ambiente do IBM Spectrum Protect Plus?.....	136
Como reparar um vSnap de origem com falha em um ambiente do IBM Spectrum Protect Plus?.....	137
Como reparar um vSnap de destino com falha em um ambiente IBM Spectrum Protect Plus?	141
Como reparar um vSnap de dupla função com falha em um ambiente do IBM Spectrum Protect Plus?.....	145
Capítulo 5. Instalando o Suporte de Backup de Kubernetes.....	149
Pré-requisitos.....	149
Instalando e implementando imagens em Kubernetes.....	152
Desinstalando o Suporte de Backup de Kubernetes.....	157
Capítulo 6. Desiniciando para um Início Rápido.....	159
Inicie o IBM Spectrum Protect Plus.....	161
Gerenciar sites.....	162
Criar políticas de backup.....	163
Criar uma conta do usuário para o administrador do aplicativo.....	165
Incluir recursos para proteger.....	167
Incluir recursos em uma definição de tarefa.....	169
Inicie a tarefa de backup.....	171
Executar um relatório.....	172
Capítulo 7. Atualizando componentes do IBM Spectrum Protect Plus.....	173
Gerenciando Atualizações.....	173
Atualizando servidores vSnap.....	176
Atualizando o sistema operacional para um servidor vSnap físico.....	177
Atualizando o sistema operacional para um servidor vSnap virtual.....	177
Atualizando um servidor vSnap.....	178
Atualizando o dispositivo virtual IBM Spectrum Protect Plus.....	178
Etapas adicionais para atualização de máquinas virtuais em ambientes de Réplica do Hyper-V.....	180
Atualizando proxies VADP.....	181
Aplicando atualizações de disponibilidade antecipada.....	182
Capítulo 8. Configurando o ambiente do sistema.....	183
Gerenciando o armazenamento de backup secundário.....	183

Gerenciando o armazenamento em.....	183
Gerenciando o armazenamento do servidor de.....	190
Gerenciando sites.....	204
Incluindo um Site.....	204
Editando um Site.....	205
Excluindo um Site.....	206
Gerenciando servidores LDAP e SMTP.....	207
Incluindo um servidor LDAP.....	207
Incluindo um servidor SMTP.....	208
Editando configurações para um servidor LDAP ou SMTP.....	209
Excluindo um servidor LDAP ou SMTP.....	210
Efetuatingo Logon no Console Administrativo.....	210
Gerenciando Chaves e Certificados.....	211
Incluindo uma chave de acesso.....	211
Excluindo uma chave de acesso.....	211
Incluindo um Certificado.....	212
Excluindo um Certificado.....	212
Incluindo uma chave SSH.....	212
Excluindo uma chave SSH.....	214
Fazendo upload de um certificado SSL a partir do console administrativo.....	214
Configurando o fuso horário.....	215
Efetuatingo logon no dispositivo virtual.....	216
Acessando o dispositivo virtual no VMware.....	216
Acessando o dispositivo virtual no Hyper-V.....	216
Testando a conectividade de rede.....	217
Executando a Ferramenta de serviço por meio de uma linha de comandos.....	217
Executando a Ferramenta de Serviço remotamente.....	218
Incluindo discos virtuais.....	219
Incluindo um disco no dispositivo virtual.....	219
Incluindo capacidade de armazenamento de um novo disco para o volume do dispositivo.....	220
Configurando preferências globais.....	222
Removendo o ambiente da Demo.....	229

Capítulo 9. Gerenciando Políticas SLA para Operações de Backup.....233

Resumo de Proteção.....	233
Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos.....	236
Criando uma política de SLA para instâncias do Amazon EC2.....	241
Criando uma política de SLA para cluster de Kubernetes.....	242
Editando uma política de SLA.....	247
Excluindo uma política de SLA.....	247

Capítulo 10. Protegendo sistemas virtualizados.....249

VMware.....	249
Incluindo uma Instância do vCenter Server.....	249
Fazendo backup dos dados de VMware.....	253
Gerenciando proxies de backup do VADP.....	259
Restaurando Dados do VMware.....	264
Hyper-V.....	275
Incluindo um servidor Hyper-V.....	275
Fazendo Backup de Dados do Hyper-V.....	277
Restaurando dados do Hyper-V.....	281
Amazon EC2.....	288
Criando um usuário do AWS IAM.....	288
Incluindo uma conta do Amazon EC2.....	290
Fazendo backup de dados do Amazon EC2.....	291
Restaurando dados do Amazon EC2.....	293
Restaurando arquivos.....	296

Capítulo 11. Protegendo sistemas de arquivos.....	299
Windows sistemas de arquivos.....	299
Pré-requisitos para o sistemas de arquivos.....	299
Incluindo um sistema de arquivos.....	300
Fazendo backup de dados do sistema de arquivos.....	304
Restaurando Dados do sistema de arquivos	310
Capítulo 12. Protegendo os contêineres.....	317
Visão Geral.....	317
Tipos de Backup e Restauração.....	318
Políticas de SLA.....	319
Funções de Usuário.....	320
Recursos de Segurança.....	321
Protegendo clusters Kubernetes usando a interface com o usuário.....	322
Registrando um cluster de Kubernetes.....	322
Definindo tarefas de backup de acordo de nível de serviço.....	325
Restaurando dados do contêiner.....	329
Expirando sessões de tarefa de Kubernetes.....	332
Visualizando tarefas e executando relatórios.....	333
Protegendo contêineres usando comandos.....	336
Pedidos do Suporte de Backup de Kubernetes.....	336
Fazendo backup de contêineres usando a linha de comandos.....	338
Restaurando dados do contêiner usando a linha de comandos.....	348
Gerenciando tarefas de backup e restauração de contêiner.....	350
Capítulo 13. Proteger sistemas de gerenciamento de nuvem.....	357
Microsoft Office 365.....	357
Registrando com o Azure Active Directory	357
Registrando o locatário do Office 365 com IBM Spectrum Protect Plus.....	358
Logs de processo detalhados.....	360
Fazendo backup de dados do Office 365.....	360
Restaurando dados do Office 365.....	361
Capítulo 14. Protegendo bancos de dados.....	363
Db2.....	363
Pré-requisitos para o Db2.....	363
Incluindo um servidor de aplicativos Db2.....	367
Fazendo backup de dados do Db2.....	370
Restaurando Dados do Db2	377
Exchange Server.....	391
Pré-requisitos.....	391
Privilégios	391
Incluindo um servidor de aplicativos do Exchange.....	393
Fazendo backup de bancos de dados do Exchange.....	394
Estratégia de Backup Incremental Contínuo.....	398
Restaurando bancos de dados do Exchange.....	398
Acessando arquivos de banco de dados do Exchange com o modo de acesso instantâneo.....	430
MongoDB.....	433
Pré-requisitos para o MongoDB.....	433
Incluindo um servidor de aplicativos MongoDB.....	436
Fazendo backup de dados do MongoDB.....	440
Restaurando Dados do MongoDB	445
Oracle.....	462
Incluindo um servidor de aplicativos Oracle.....	462
Fazendo Backup de Dados do Oracle.....	464
Restaurando dados do Oracle.....	467

SQL Server.....	474
Incluindo um servidor de aplicativos SQL Server.....	475
Fazendo Backup dos Dados do SQL Server.....	477
Restaurando os Dados do SQL Server.....	481
Capítulo 15. Protegendo IBM Spectrum Protect Plus.....	491
Fazendo Backup do Aplicativo.....	491
Restaurando o aplicativo.....	491
Gerenciando pontos de restauração.....	492
Expirando sessões de tarefa.....	492
Excluindo metadados de recursos do catálogo.....	493
Capítulo 16. Gerenciando tarefas e operações.....	495
Tipos de Tarefa.....	495
Criando tarefas e programações de tarefas.....	496
Iniciando tarefas sob demanda.....	497
Visualizando Tarefas.....	498
Visualizando o progresso da tarefa de backup no nível de recursos.....	499
Visualizar Logs de Tarefa.....	500
Visualizando tarefas simultâneas.....	500
Pausando e Continuando Tarefas.....	501
Editando tarefas e planejamentos de tarefa.....	501
Cancelando Tarefas.....	502
Excluindo tarefas.....	502
Executando novamente as tarefas de backup parcialmente concluídas.....	502
Executando uma tarefa de backup ad hoc.....	503
Configurando scripts para operações de backup e restauração.....	504
Fazendo Upload de um Script.....	504
Incluindo um script em um servidor.....	504
Capítulo 17. Gerenciando relatórios e logs.....	507
Tipos de relatório.....	507
Relatórios de Utilização de Armazenamento de Backup.....	507
Relatórios de proteção.....	508
Relatórios do sistema.....	511
Executando relatórios de ambiente da VM.....	512
Relatar Ações.....	514
Executando um relatório.....	514
Criando um Relatório Customizado.....	515
Planejando um relatório.....	515
Coletando e revisando logs de auditoria para ações.....	516
Capítulo 18. Gerenciando o acesso de.....	517
Gerenciando grupos de recursos do usuário.....	517
Criando um Grupo de Recursos.....	518
Editando um Grupo de Recursos.....	521
Excluindo um Grupo de Recursos.....	521
Gerenciando atribuições.....	521
Criando uma função.....	523
Editando uma função.....	525
Excluindo uma função.....	526
Gerenciando contas do usuário.....	526
Criando uma conta do usuário para um usuário individual.....	526
Criando uma conta do usuário para um grupo LDAP.....	526
Editando as credenciais da conta do usuário.....	527
Excluindo uma Conta do Usuário.....	528
Gerenciando identidades.....	528

Incluindo uma Identidade.....	528
Editando uma Identidade.....	528
Excluindo uma Identidade.....	529
Capítulo 19. Visão geral do licenciamento.....	531
Tags do Software License Metric (SLM).....	531
Integração com o IBM License Metric Tool (ILMT).....	532
Capítulo 20. Detecção de problemas.....	533
Coletando Arquivos de Log para Resolução de Problemas.....	533
Como criar camadas de dados para o armazenamento em fita ou em nuvem?	533
Resolução de Problemas do Suporte de Backup de Kubernetes.....	534
Coletando arquivos de log do Suporte de Backup de Kubernetes.....	534
Configurando o nível de rastreio de arquivos de log.....	535
Visualizando logs de rastreio para Suporte de Backup de Kubernetes.....	536
Referência Rápida.....	537
Resolução de problemas de backups e restaurações.....	541
Capítulo 21. Mensagens do produto.....	549
Prefixos de mensagem.....	549
Apêndice A. Diretrizes de Procura.....	551
Apêndice B. Acessibilidade.....	553
Avisos.....	555
Glossário.....	559
Índice Remissivo.....	561

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 23.

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 10.1.6

IBM Spectrum Protect Plus Versão 10.1.6 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](#).

Se houver mudanças na documentação, elas serão indicadas por uma barra vertical (|) na margem.

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

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.

IBM Spectrum Protect Plus pode ser implementado como uma solução independente ou integrada com armazenamento em nuvem ou um servidor de repositório, como um Servidor IBM Spectrum Protect para armazenamento de dados de longo prazo.

Storyboard de implementação para IBM Spectrum Protect Plus

Este storyboard pode ajudá-lo a executar as tarefas que são necessárias para implementar o produto. O *storyboard de implementação* foi projetado para ajudá-lo a implementar o IBM Spectrum Protect Plus com sucesso em um ambiente de produção. O storyboard lista cada tarefa na sequência necessária e fornece links para instruções de tarefa, vídeos e diretrizes no IBM Spectrum Protect Plus Blueprints. O storyboard descreve o resultado esperado de tarefas para que você possa verificar o seu progresso à medida que você implanta o produto.

Antes de você iniciar, revise os requisitos do sistema para o seu ambiente. Para obter mais informações, consulte “Requisitos de Sistema” na página 23.

As etapas na [Tabela 1](#) contam com as informações no [Blueprints](#) e com o funcionamento da ferramenta *Sizer*. Os links de vídeo são fornecidos na [Tabela 2](#) para ajudá-lo com essas tarefas.

Tabela 1. Storyboard de implementação		
História	Procedimento	Resultado esperado
Prepare-se para dimensionar os requisitos de sua capacidade, baixando o Blueprints e a planilha do Sizer Tool.	<p>Para obter diretrizes de dimensionamento, consulte os Capítulos 1-3 do IBM Spectrum Protect Plus Blueprints.</p> <p>Para obter ajuda com o uso da planilha de dimensionamento, consulte os links de vídeo na Tabela 2.</p> <p>Faça o download do <i>Sizer Tool</i>, que é uma planilha de dimensionamento, na página a seguir e conclua as seguintes etapas: Blueprints.</p>	Você tem a planilha do Sizer Tool e as informações necessárias para dimensionar seus requisitos de capacidade do IBM Spectrum Protect Plus.

Tabela 1. Storyboard de implementação (continuação)

História	Procedimento	Resultado esperado
<p>Dimensione a capacidade que é necessária para o armazenamento primário em seu ambiente.</p>	<p>Use o Sizer para dimensionar o armazenamento primário.</p> <ol style="list-style-type: none"> 1. Abra a planilha do <i>Sizer Tool</i> transferida por download e ative macros. Salve uma cópia da planilha em sua unidade local para armazenamento primário. 2. Preencha a planilha Iniciar Aqui especificando suas escolhas para opções globais para o armazenamento primário. 3. Abra a guia VMware e insira dados para a capacidade do vCenter que inclui a mudança de taxa diária e o crescimento anual. 4. Abra a guia HyperV e insira dados para sua capacidade de HyperV. 5. Para cada aplicativo que você está planejando usar, abra uma guia de aplicativos e insira dados para suas necessidades de capacidade. 6. Quando todos os dados forem inseridos, clique na guia Resultados do Dimensionamento para revisar os resultados calculados. 7. Configure o tamanho do servidor vSnap preferencial. Para especificar automaticamente o valor para o tamanho do conjunto de armazenamento vSnap, clique em Automático. 8. Insira a porcentagem de reserva do servidor vSnap necessária. Essa reserva é a porcentagem do armazenamento do servidor vSnap que é reservada para uso, operações de restauração e para qualquer reutilização. 9. Abra IBM Spectrum Protect Plus e navegue até Configuração do Sistema > Preferências Globais. Insira as porcentagens de preferências globais, conforme mostrado no <i>Sizer Tool</i>. Use essas porcentagens para configurar as opções a seguir: <ul style="list-style-type: none"> • Erro de espaço livre de destino (porcentagem) • Aviso de espaço livre de destino (porcentagem) 10. Revise os resultados do Sizer para seu armazenamento primário. Salve o Sizer, mas deixe aberto para inserir configurações que são necessárias para o armazenamento secundário. 	<p>A planilha do Sizer Tool ajuda você a calcular as informações de dimensionamento do armazenamento primário.</p> <p>Você salvou uma cópia da planilha de dimensionamento do Sizer. Se os requisitos de capacidade mudarem, é possível atualizar a planilha de acordo.</p> <p>Você também tem detalhes sobre o número e o tamanho necessários dos servidores vSnap e, opcionalmente, o número de API de vStorage do VMware necessários para proxies de proteção de dados.</p> <p>Você tem detalhes sobre uma visão de oito anos de crescimento com base em sua entrada na planilha. Você configura preferências globais para acionamento de aviso e erros do vSnap quando ele atinge um limite especificado com base no uso de porcentagem.</p>

Tabela 1. Storyboard de implementação (continuação)

História	Procedimento	Resultado esperado
<p>Dimensione a capacidade necessária para o armazenamento secundário em seu ambiente.</p>	<p>Use o Sizer para dimensionar o armazenamento secundário seguindo estas etapas. Consulte o Capítulo 5 do Blueprints.</p> <ol style="list-style-type: none"> 1. Faça o download da planilha de dimensionamento a partir da página Blueprints e ative macros. Salve uma cópia da planilha do Sizer para sua unidade local para armazenamento secundário. 2. Se houver algum valor, reconfigure a planilha do <i>Sizer Tool</i> clicando em Clicar para Reconfigurar. 3. Preencha a planilha Iniciar Aqui especificando suas escolhas para opções globais para o armazenamento secundário. 4. Acesse a guia Resultados da planilha do <i>Sizer Tool</i> do armazenamento primário que você salvou anteriormente. Copie os resultados que estão listados na tabela de carga de trabalho Replicação e insira os valores na tabela Carga de Trabalho de Entrada de Replicação Opcional na guia Iniciar Aqui da planilha do Sizer Tool de armazenamento secundário. 5. Se você pretende proteger os dados do aplicativo, conclua as guias do aplicativo. Por exemplo, é possível especificar opções de cópia de dados para políticas de armazenamento e replicação de objetos. 6. Revise os resultados de dimensionamento para seu armazenamento secundário. Salve e feche as planilhas do Sizer Tool. 	<p>Você tem o dimensionamento para a capacidade para o armazenamento secundário para o seu ambiente do IBM Spectrum Protect Plus.</p> <p>Você salvou uma cópia do Sizer para o armazenamento secundário em seu ambiente. Se alguma coisa mudar, você pode alterar o Sizer e fazer mudanças conforme necessário.</p> <p>Você também tem detalhes sobre a quantidade de servidor vSnap para cada ano, a quantidade de proxy VADP e o tamanho de cada servidor vSnap.</p> <p>Você tem detalhes de uma visão de oito anos de crescimento com base em suas entradas no Sizer. Você configura preferências globais para acionamento de aviso e erros do vSnap quando ele atinge uma porcentagem de uso.</p>
<p>Instale ou faça o upgrade do IBM Spectrum Protect Plus usando a imagem ISO para a versão que você requer. Se você atualizar o ambiente do sistema, um novo kernel será instalado e a reinicialização será necessária.</p>	<p>Instale o IBM Spectrum Protect Plus, siga as instruções em “Instalando o IBM Spectrum Protect Plus como um dispositivo virtual VMware” na página 99 ou “Instalando o IBM Spectrum Protect Plus como um dispositivo virtual Hyper-V” na página 101.</p>	<p>O IBM Spectrum Protect Plus é instalado.</p>

Tabela 1. Storyboard de implementação (continuação)		
História	Procedimento	Resultado esperado
Instale ou faça o upgrade do servidor vSnap usando a imagem ISO para a versão que você requer. Se você estiver usando a deduplicação de dados, a reinicialização do servidor vSnap pode levar até 15 minutos.	Instale o servidor vSnap e siga as instruções em “Instalando um servidor vSnap físico” na página 109. Se você estiver instalando um servidor vSnap virtual, siga as instruções em “Instalando um servidor vSnap virtual em um ambiente Hyper-V” na página 112.	O servidor vSnap está instalado. Para verificar se o servidor vSnap está instalado, execute o comando <code>vsnap show</code> .
Construa o servidor vSnap com a capacidade que você derivou do dimensionamento usando o Blueprints e o <i>Sizer Tool</i> .	<ol style="list-style-type: none"> 1. Crie volumes e mapeia dispositivos vSnap. 2. Mapeie volumes para o cluster da VM. 3. Consulte as etapas para configuração de um servidor vSnap virtual ou físico no Blueprints, Blueprints. 	O servidor vSnap é construído.
Inclua o espaço de log.	<p>Crie um driver de Múltiplos Dispositivos do Linux® com três partições para armazenar o cache de armazenamento do servidor vSnap, cache de nuvem e arquivos de log. Para o cache de nuvem, a capacidade é configurada em 128 GB por padrão. Se você pretende copiar dados na nuvem, deve-se aumentar a capacidade. Para os servidores de vSnap físicos copiarem dados para o armazenamento em nuvem, deve-se criar o sistema de arquivos <code>/opt/vsnap-data</code> com a capacidade necessária.</p> <p>Para obter mais informações sobre esta etapa, consulte <i>Configurando um servidor de vSnap físico usando RAID fornecido por software de armazenamento</i> e <i>Capítulo 7 Configurando o Cloud Object Storage</i> no Blueprints.</p>	Você configurou espaço de log para seus servidores vSnap virtuais ou físicos.
Registre o servidor vSnap.	Registre o servidor vSnap. Para obter mais informações e etapas, consulte “Registrando um servidor vSnap como um provedor de armazenamento de backup” na página 115.	O servidor vSnap é registrado e incluído no IBM Spectrum Protect Plus.
Inicialize o servidor vSnap.	Depois de instalar ou fazer o upgrade do IBM Spectrum Protect Plus, e incluir servidores vSnap, deve-se inicializar os servidores vSnap. Para obter informações e etapas, consulte “Concluindo uma inicialização simples” na página 127.	Dependendo da sua escolha, o servidor vSnap é inicializado com ou sem criptografia.
Configure o servidor vSnap.	Para configurar opções de armazenamento do servidor vSnap, como incluir parceiros de replicação, consulte “Configurando opções de armazenamento de backup” na página 118.	Se você configurou o recurso de replicação de dados, os parceiros de replicação serão configurados.

Tabela 1. Storyboard de implementação (continuação)		
História	Procedimento	Resultado esperado
(Opcional) Configure o servidor vSnap como um proxy VADP.	Se você estiver usando um proxy VADP para otimizar a movimentação de dados para e do servidor vSnap, deve-se registrar o servidor vSnap como um proxy VADP. Para obter mais instruções, consulte “Registrando um proxy VADP em um servidor vSnap” na página 262.	O servidor vSnap é configurado como um proxy VADP.
Configure o ambiente VMware que inclui a criação de um vCenter e o registro de um hypervisor.	Para proteger os dados do VMware, deve-se primeiro configurar um vCenter Server. Para obter instruções, consulte “Fazendo Backup e Restaurando Dados do VMware” na página 249. Assegure-se de que os privilégios necessários do vCenter Server estejam ativados. Para obter mais informações sobre os privilégios necessários, consulte “Privilégios de máquina” na página 250.	Um vCenter é configurado com as permissões necessárias para que você possa começar a proteger os dados do VMware.
Incluir Usuários.	Inclua os usuários que serão necessários para usar IBM Spectrum Protect Plus. Para obter mais informações, consulte “Criando uma conta do usuário para um usuário individual” na página 526 usando o formulário Incluir Usuário na página.	Os usuários são incluídos e recebem permissões para operar o IBM Spectrum Protect Plus.
Crie uma política de acordo de nível de serviço (SLA).	Configure uma política ou políticas de SLA para as suas cargas de trabalho do IBM Spectrum Protect Plus. Para obter informações adicionais sobre políticas de ANS, consulte Capítulo 9, “Gerenciando Políticas SLA para Operações de Backup” , na página 233.	As políticas de SLA para suas cargas de trabalho IBM Spectrum Protect Plus são configuradas e você está pronto para executar tarefas de backup.
Atualize as preferências globais.	Os administradores podem editar as preferências globais para todas as operações como deduplicação ou criptografia. Para obter informações adicionais sobre preferências globais, consulte “Configurando preferências globais” na página 222.	Se as preferências globais forem configuradas, elas se aplicarão a todo o ambiente do IBM Spectrum Protect Plus.

Recursos e biblioteca de vídeos

Os blueprints devem ser usados para dimensionar seu ambiente do IBM Spectrum Protect Plus. Os vídeos que estão listados na tabela [Tabela a](#) seguir podem ajudá-lo com esse processo.

Tabela 2. Blueprints e dimensionamento	
Tarefa ou tópico	Link de vídeo
Introdução ao Sizer Tool	IBM Spectrum Protect Plus Sizer and Blueprints: 1. Sizer introduction - Demo
Visão geral da planilha do Sizer	IBM Spectrum Protect Plus Sizer & Blueprints: 2. Sizer Worksheet Overview – Demo
Valores globais do Sizer	IBM Spectrum Protect Plus Sizer & Blueprints: 3. Sizer Global Values – Demo
Incluindo um hypervisor	IBM Spectrum Protect Plus Sizer & Blueprints: 4. Adding a Hypervisor workload to the sizer – Demo
Adicionando um Aplicativo	IBM Spectrum Protect Plus Sizer & Blueprints: 5. Adding Application workload to the sizer– Demo

Tabela 2. Blueprints e dimensionamento (continuação)	
Tarefa ou tópico	Link de vídeo
Avaliando os resultados	IBM Spectrum Protect Plus Sizer & Blueprints: 6. Evaluating the sizer's results – Demo
Incluindo armazenamento secundário	IBM Spectrum Protect Plus Sizer & Blueprints: 7. Adding a secondary site to sizer – Demo
Cenários <i>What if</i>	IBM Spectrum Protect Plus Sizer & Blueprints: 8. What if sizing scenarios – Demo
O que há de novo nos blueprints	IBM Spectrum Protect Plus Sizer & Blueprints: 9. What's new in 10.1.5 sizer – Presentation
Usando os resultados do Sizer para implementação	IBM Spectrum Protect Plus Sizer & Blueprint: 10. Tying the blueprints, sizer and install together - Demo

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 serviço IBM Spectrum Protect Plus em uma implementação, mesmo que a implementação seja difundida para 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 8.

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

Item	Descrição
Ícone do IBM Spectrum Protect 	Este ícone abre IBM Spectrum Protect Operations Center para fornecer proteção de dados expandida. Este ícone está ativo apenas quando a URL é inserida no campo de preferência URL do Centro de Operações do IBM Spectrum Protect na página Preferências Globais . Para obter informações sobre essa preferência, consulte “Configurando preferências globais” na página 222.
Ícone Alertas 	Este ícone abre a janela Alertas . Para obter mais informações sobre alertas, consulte “Alertas” na página 10.
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.

Restrição: O produto IBM Spectrum Protect Plus não segue classificação de ordenação de ICU para menus, portanto, a ordenação de menus aparecerá em ordem de ponto de código. Por exemplo, alguns idiomas classificam letras de forma diferente da ordem de ponto de código. Como tal, a ordem classificada dos caracteres e das palavras como eles aparecem nos menus ao usar esses idiomas aparecerá fora da ordem esperada.

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.

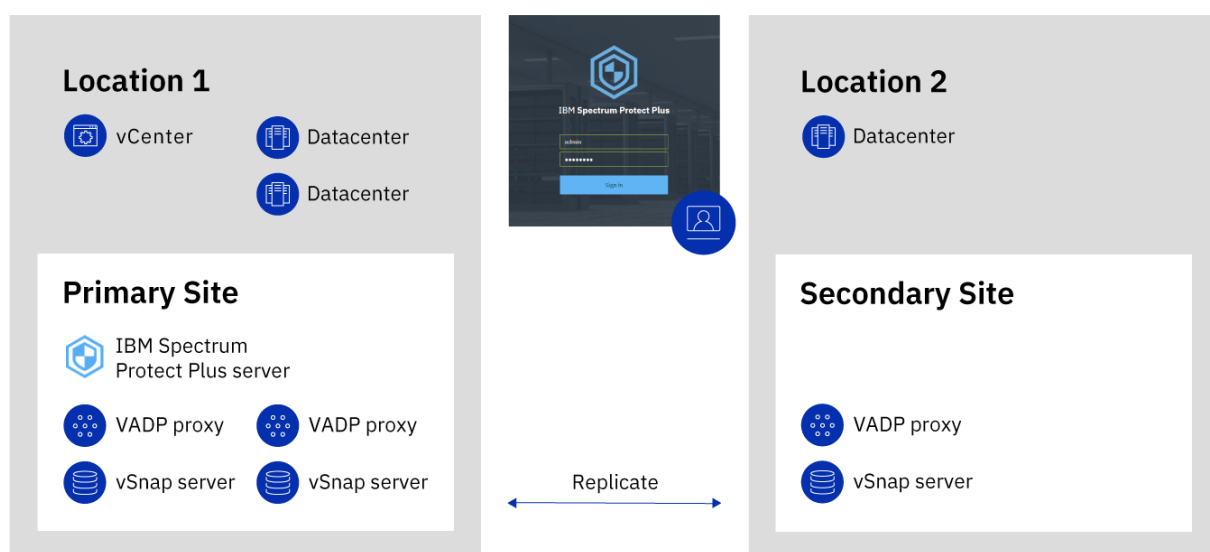


Figura 1. IBM Spectrum Protect Plus implementação em duas localizações geográficas

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 as 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 a economia de espaço alcançada além da 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.

Políticas

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 quantia de espaço livre em disco é 10% ou menos.

espaço de armazenamento vSnap baixo

É exibido quando a quantia 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 captura instantânea de armazenamento de cópia bloqueada

É exibido quando a captura instantânea de armazenamento copiada mais recentemente é bloqueada. Aumente a retenção de cópia ou aumente a política de frequência de cópia.

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 quantia de espaço restante.

Deduplicação desativada no armazenamento

É exibido quando a deduplicação é desativada e exibe o IP do servidor de armazenamento. Isso ocorrerá quando a opção de desativação automática da tabela de deduplicação (DDT) do vSnap estiver ativada e o tamanho ou limite de porcentagem definido for excedido.

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 18, “Gerenciando o acesso de”, na página 517](#).

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 9, “Gerenciando Políticas SLA para Operações de Backup”, na página 233](#).

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:

- Em ambientes que contêm mais de um servidor vSnap, todos os servidores vSnap devem ter uma parceria estabelecida.
- 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.

Copiar capturas instantâneas 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 copiar capturas instantâneas de um servidor vSnap para o armazenamento de backup secundário.

Mudança na terminologia: Em liberações anteriores, o processo de cópia de dados do IBM Spectrum Protect Plus para o armazenamento de backup secundário era conhecido como *transferência* de dados. A partir do IBM Spectrum Protect Plus Versão 10.1.5, o processo é conhecido como *cópia* de dados.

Os seguintes destinos de armazenamento de backup secundário estão disponíveis para operações de cópia:

- 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 objetos padrão

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

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

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

Armazenamento de archive em fita ou nuvem

O armazenamento em fita significa que os dados são armazenados na mídia de fita física ou Virtual Tape Library (VTL). O armazenamento em fita é uma opção quando você copia dados de captura instantânea para um Servidor IBM Spectrum Protect.

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 copia dados de captura instantânea para fita ou para um sistema de armazenamento em nuvem, uma cópia completa dos dados é criada.

Copiar capturas instantâneas para o armazenamento de archive de objeto em fita ou em nuvem fornece benefícios extras de custo e segurança. 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. No entanto, como a cópia para esses tipos de armazenamento requer uma cópia de dados completa, 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.

Quando você estiver copiando dados para fita do IBM Spectrum Protect Plus para o Servidor IBM Spectrum Protect, não será uma boa ideia usar a função hierárquica do IBM Spectrum Protect. Se você estiver arquivando dados para fita, deverá usar um conjunto de armazenamentos em cache frio. Para obter mais informações sobre a criação de camadas, consulte [“Como criar camadas de dados para o armazenamento em fita ou em nuvem?”](#) na página 533. Para diferentes cenários e mais informações sobre como configurar o armazenamento, consulte [“Configuração para copiar ou arquivar dados para IBM Spectrum Protect”](#) na página 190.

Para obter informações sobre como os dados de captura instantânea são copiados para o armazenamento de objeto padrão e armazenamento de objeto de archive para cada sistema de armazenamento em nuvem, consulte [“Requisitos de armazenamento em nuvem”](#) na página 37.

Incluindo armazenamento de backup secundário e criando políticas de backup

Para copiar capturas instantâneas para o armazenamento secundário, as ações a seguir são necessárias:

Ação	Como
Para copiar capturas instantâneas para um servidor de repositório <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.	Consulte “Configuração para copiar ou arquivar dados para IBM Spectrum Protect” na página 190 e “Registrando um servidor de repositório como um provedor de armazenamento de backup” na página 202.
Para copiar capturas instantâneas para armazenamento em nuvem, inclua o armazenamento em IBM Spectrum Protect Plus.	Siga as instruções para seu tipo de armazenamento selecionado: <ul style="list-style-type: none">• “Incluindo o Armazenamento de objeto do Amazon S3” na página 184• “Incluindo o IBM Cloud Object Storage como um provedor de armazenamento de backup” na página 185• “Incluindo armazenamento em nuvem do Microsoft Azure como um provedor de armazenamento de backup” na página 187• “Registrando um servidor de repositório como um provedor de armazenamento de backup” na página 202
Crie uma política de backup que inclua o armazenamento.	Consulte “Criar políticas de backup” na página 163.

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 copiadas do servidor vSnap no site secundário para o armazenamento em nuvem para proteção de dados de longo prazo.

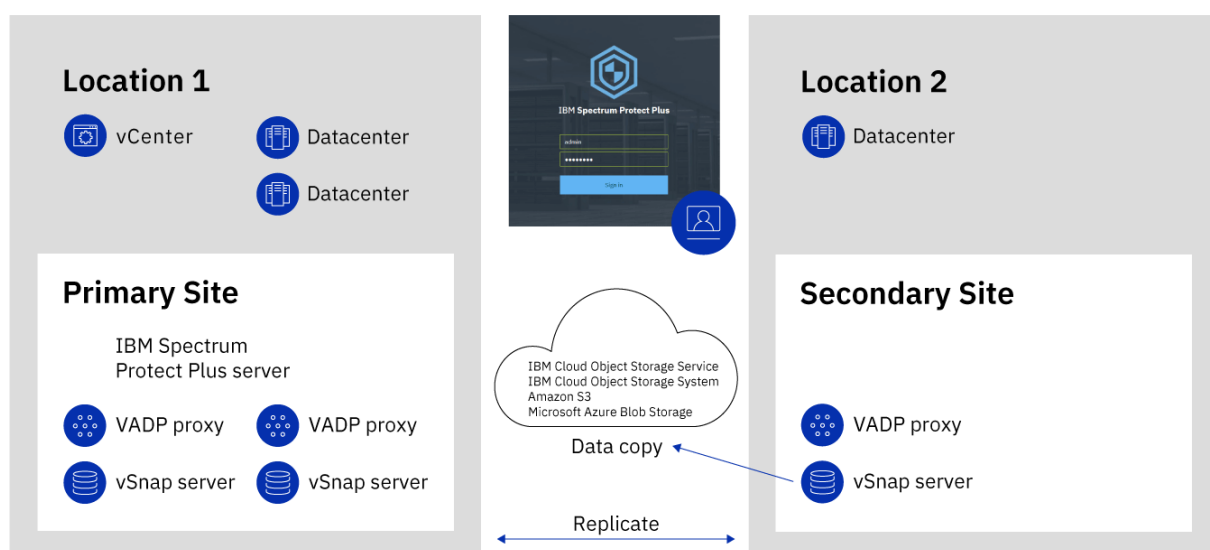


Figura 2. Implementação do IBM Spectrum Protect Plus em duas localizações geográficas com cópia para armazenamento em nuvem

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

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

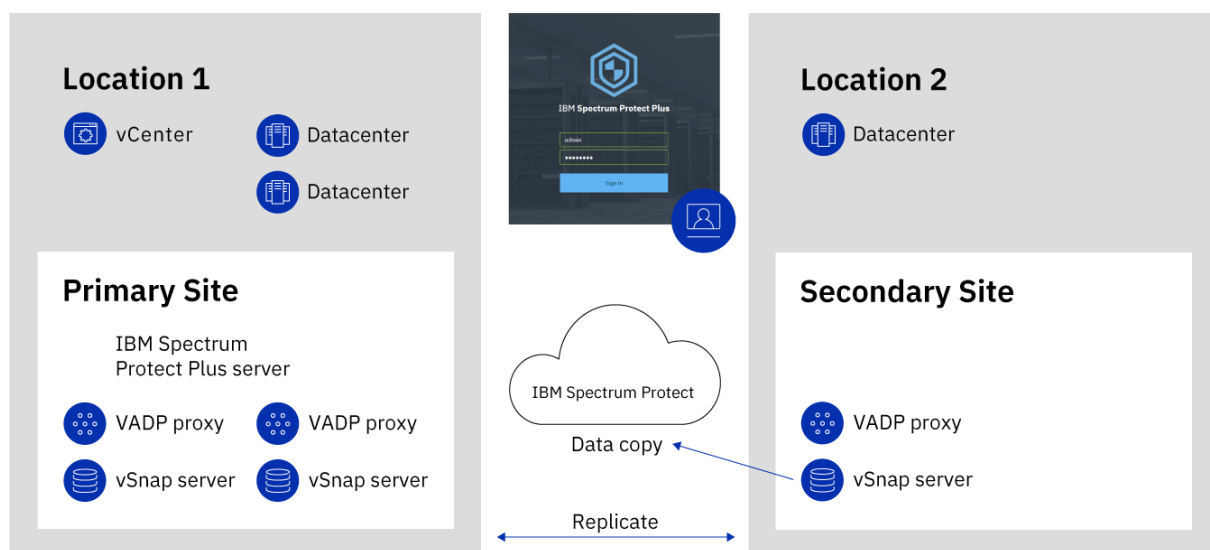


Figura 3. Implementação do IBM Spectrum Protect Plus em duas localizações geográficas com cópia para IBM Spectrum Protect

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

IBM Spectrum Protect Plus na plataforma em nuvem do Amazon Web Services (AWS) é uma solução de proteção de dados para usuários que desejam proteger bancos de dados que estão em execução no AWS. Além disso, os usuários podem proteger máquinas virtuais que são gerenciadas pelo VMware Cloud (VMC) no AWS, enquanto têm o servidor IBM Spectrum Protect Plus instalado no VMC e o servidor vSnap instalado em uma VPC (Nuvem Particular Virtual) do AWS.

É possível implementar IBM Spectrum Protect Plus on AWS em uma das configurações a seguir. O suporte para o VMC no AWS está disponível apenas em um ambiente híbrido. Para obter mais informações sobre o suporte para o VMC no AWS, consulte [IBM Spectrum Protect Plus for VMware Cloud no AWS](#).

Ambiente all-on-cloud

Nessa configuração, tanto o servidor IBM Spectrum Protect Plus quanto o servidor vSnap são implementados no AWS em uma VPC existente ou nova. Um servidor IBM Spectrum Protect Plus no local e uma infraestrutura VMware ou Microsoft Hyper-V não são necessários.

Essa opção pode beneficiar novos usuários do IBM Spectrum Protect Plus que desejam proteger bancos de dados no AWS e não têm o IBM Spectrum Protect Plus em execução em um ambiente no local.

Ambiente híbrido

Nessa configuração, apenas o servidor vSnap é implementado no AWS em uma VPC existente ou nova. O servidor IBM Spectrum Protect Plus é instalado e mantido no local ou em outro local. Essa opção pode beneficiar os usuários do IBM Spectrum Protect Plus existentes que desejam continuar protegendo cargas de trabalho que estão em execução no local e no ambiente em nuvem.

Além das operações de backup e recuperação, você também pode utilizar um ambiente híbrido para replicar e reutilizar dados entre uma localização no local e o AWS para proteção adicional de dados. Por exemplo, você pode querer usar dados que são protegidos em seu site no local no AWS for DevOps, garantia de qualidade, testes e propósitos de recuperação de desastres.

Implementando o IBM Spectrum Protect Plus no AWS

O [Página do IBM Spectrum Protect Plus](#) no AWS Marketplace fornece os modelos AWS CloudFormation que são necessários para implementar o servidor IBM Spectrum Protect Plus e o servidor vSnap no AWS, bem como informações de 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.

Integração com o IBM Spectrum Protect

É possível monitorar seu ambiente IBM Spectrum Protect Plus a partir de IBM Spectrum Protect Operations Center. Por conveniência, você também pode acessar o Operations Center diretamente a partir de IBM Spectrum Protect Plus.

Monitore IBM Spectrum Protect Plus a partir do Operations Center

O Operations Center inclui um painel para IBM Spectrum Protect Plus que fornece as seguintes informações:

- Um resumo das atividades de tarefa para um período selecionado. É possível visualizar os percentuais de backup, restauração e outras tarefas que foram bem-sucedidas e que falharam. Nessas informações resumidas, é possível acessar informações mais detalhadas para cada tipo de tarefa.
- Um resumo da capacidade e disponibilidade de servidores vSnap. É possível visualizar a capacidade total do disco que está disponível para o servidor IBM Spectrum Protect Plus por meio de todos os servidores vSnap. Também é possível visualizar a capacidade disponível para cada servidor vSnap.
- Um resumo das políticas do acordo de nível de serviço (SLA) que são definidas no servidor IBM Spectrum Protect Plus. É possível visualizar o número de políticas que têm tarefas de backup associadas. Também é possível visualizar a porcentagem de recursos que são protegidos por tarefas de backup e o número de recursos que não são protegidos. Por meio dessas informações de resumo, é possível acessar as informações de política mais detalhadas.

Para ativar esse recurso, um administrador do sistema deve incluir o servidor IBM Spectrum Protect Plus no Operations Center.

Acesse o Operations Center a partir da GUI IBM Spectrum Protect Plus

Para acessar o Operations Center a partir do IBM Spectrum Protect Plus, um administrador do sistema deve incluir a URL do Operations Center na página **Preferências Globais** da GUI do IBM Spectrum Protect Plus.

Em seguida, é possível acessar o Operations Center a partir do ícone IBM Spectrum Protect na barra de menus.

Incluindo IBM Spectrum Protect Plus no Operations Center

Quando você inclui um servidor IBM Spectrum Protect Plus no Operations Center, você estabelece uma conexão entre o servidor e o Operations Center. Depois que essa conexão for estabelecida, é possível usar o Operations Center para monitorar o ambiente IBM Spectrum Protect Plus.

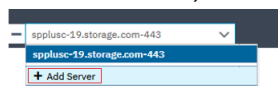
Antes de Iniciar

Assegure-se de que você tenha a URL para o Operations Center e as credenciais do usuário para efetuar login.

Procedimento

Para incluir um servidor IBM Spectrum Protect Plus no Operations Center, conclua as etapas a seguir:

1. Na barra de menus do Operations Center, clique em **Visões Gerais > Protect Plus** e tome uma das ações a seguir para abrir o assistente **Incluir Servidor**:

Configuração atual	Ação
Nenhum servidor IBM Spectrum Protect Plus está conectado ao Operations Center.	Uma mensagem indica que nenhum servidor IBM Spectrum Protect Plus está configurado. Clique em + Incluir Servidor .
Um ou mais servidores IBM Spectrum Protect Plus estão conectados ao Operations Center.	O painel do IBM Spectrum Protect Plus é exibido. A partir da lista de servidores no painel de monitoramento, selecione + Incluir Servidor 

2. Para incluir o servidor IBM Spectrum Protect Plus, siga as orientações no assistente.

Na página **Autorização** do assistente, é solicitado que você especifique credenciais do usuário para acessar e monitorar o servidor IBM Spectrum Protect Plus. Se você tiver uma conta IBM Spectrum Protect Plus cujas credenciais combinam com as credenciais do Operations Center, será possível usar essa conta. Se você não tiver credenciais correspondentes, deve-se criar uma conta.

Usar credenciais do Operations Center

Selecione esta opção para usar uma conta do usuário do IBM Spectrum Protect Plus existente que corresponda ao nome do usuário e à senha da conta do administrador que você usou para efetuar login no Operations Center.

Criar uma conta de usuário de monitoramento

Selecione esta opção para que o assistente crie uma conta do usuário do IBM Spectrum Protect Plus.

Para permitir que o Operations Center acesse o IBM Spectrum Protect Plus e crie a conta, forneça credenciais para uma conta do usuário do IBM Spectrum Protect Plus que é designada à função SYSADMIN. Insira as credenciais nos campos **Nome de Usuário** e **Senha**, conforme mostrado na figura a seguir.

Add Server

Authorization

Identify or create a user account on the IBM Spectrum Protect Plus server for monitoring. [Learn more](#)

☐ Use Operations Center credentials (User account with the same credentials must already be defined on server)

☒ Create a monitoring administrator

Specify IBM Spectrum Protect Plus login credentials for a user account that can create custom user roles and user accounts. This user account is used only during configuration. During configuration, a new user role and account for monitoring are created.

User name

Password

Back

Add Server

Cancel


Figura 4. Inserindo credenciais do IBM Spectrum Protect Plus

As credenciais que são inseridas aqui não são salvas. O Operations Center efetua logon no servidor IBM Spectrum Protect Plus usando essas credenciais de conta e cria a conta do usuário `OC_MONITOR_number`, em que *number* é um número aleatório para identificação. O Operations Center irá se conectar ao ambiente do IBM Spectrum Protect Plus usando a nova conta.

3. Clique em **Add Server**.

Se a operação for bem-sucedida, os resultados serão exibidos, conforme mostrado na figura a seguir:

Add Server

 Succeeded

10:19 PM Adding IBM Spectrum Protect Plus server...
Connecting to the IBM Spectrum Protect Plus server.
Creating monitor role.
Creating monitor user.
Saving server.
Establishing session.







Close


Figura 5. IBM Spectrum Protect Plus incluído com sucesso

Inserindo a URL do Operations Center

Para acessar o Operations Center a partir de IBM Spectrum Protect Plus, insira a URL para o Operations Center nas preferências globais do IBM Spectrum Protect Plus.

Sobre Esta Tarefa

Você deve ter as credenciais do administrador do IBM Spectrum Protect Plus para configurar preferências globais.

Quando essa preferência é inserida, o ícone do IBM Spectrum Protect  fica ativo na barra de menus do IBM Spectrum Protect Plus.

Procedimento

Para inserir a URL para o Operations Center, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Configuração do sistema > Preferências globais**.
2. Insira a URL para o Operations Center no campo **URL do IBM Spectrum Protect Operations Center**.

Global Preferences

Register system preferences for your IBM Spectrum Protect Plus environment.

Integration with other storage products

IBM Spectrum Protect Operations Center



<https://tapsrv09.storage.tucson.il>



URL

Figura 6. Inserindo a URL do Operations Center

3. Para ativar o ícone do IBM Spectrum Protect na barra de menus IBM Spectrum Protect Plus, efetue logoff no IBM Spectrum Protect Plus e depois logon novamente.

Acessando o Operations Center

Inicie o Operations Center para monitorar seu ambiente IBM Spectrum Protect Plus .


Antes de Iniciar

Assegure-se de que as etapas a seguir sejam concluídas:

- “Incluindo IBM Spectrum Protect Plus no Operations Center” na [página 17](#)
- “Inserindo a URL do Operations Center” na [página 19](#)

Procedimento

Para acessar o Operations Center e monitorar o seu ambiente do IBM Spectrum Protect Plus, complete as seguintes etapas:

1. Na barra de menus do IBM Spectrum Protect Plus, clique no ícone IBM Spectrum Protect .
2. Efetue login no Operations Center.
3. Na barra de menus do Operations Center, clique em **Visões Gerais > Protect Plus**.

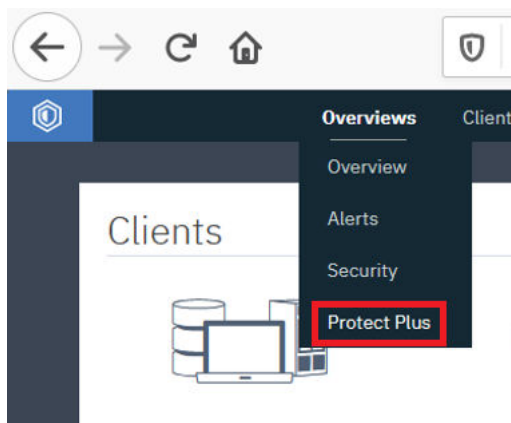


Figura 7. Selecionando IBM Spectrum Protect Plus no Operations Center

4. Visualize o status de seu ambiente do IBM Spectrum Protect Plus no painel de monitoramento IBM Spectrum Protect Plus, conforme mostrado na figura de exemplo a seguir:

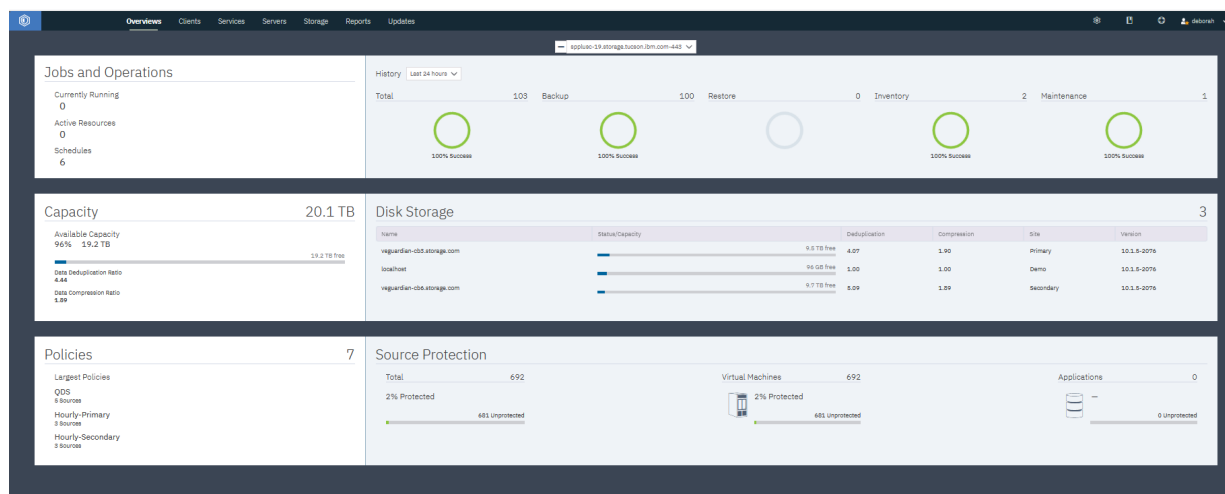


Figura 8. Visualizando o painel do IBM Spectrum Protect Plus

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 23.
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 23.
Se forem necessários servidores vSnap adicionais para suportar seu ambiente, instale e configure os servidores.	Consulte Capítulo 3, “Instalando servidores vSnap” , na página 109.
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 259.
Conclua as etapas básicas para configurar e começar a usar o IBM Spectrum Protect Plus.	Consulte Capítulo 6, “Desiniciando para um Início Rápido” , na página 159.

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 [Nota técnica 304861](#).

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 [Nota técnica 304861](#).

O suporte do IBM Spectrum Protect Plus para plataformas, aplicativos, serviços e hardware de terceiros depende de terceiros fornecedores. Quando um produto ou versão de um terceiro fornecedor entra em suporte estendido, suporte de autoatendimento ou fim de vida, IBM Spectrum Protect Plus suporta o produto ou a versão no mesmo nível que o fornecedor.

Instalação da máquina virtual

IBM Spectrum Protect Plus é instalado como um dispositivo virtual. Antes de implementar IBM Spectrum Protect Plus no host, assegure-se de que um dos requisitos a seguir seja atendido:

- 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 níveis de correção (começando com o IBM Spectrum Protect Plus V10.1.2)
- vSphere 7.0, incluindo todas as atualizações e níveis de correção (começando com o IBM Spectrum Protect Plus V10.1.6)
- Microsoft® Hyper-V 2016
- Microsoft Hyper-V 2019 (começando com o IBM Spectrum Protect Plus V10.1.3)

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

- servidor de 8-core de 64 bits
- 48 GB de memória
- 548 GB de armazenamento em disco para a máquina virtual (VM)

Use um servidor Network Time Protocol (NTP) para sincronizar o fuso horário entre os recursos do IBM Spectrum Protect Plus em seu ambiente, como o dispositivo virtual IBM Spectrum Protect Plus, matrizes de armazenamento, hypervisors e servidores de aplicativos. Se os relógios nos vários sistemas estiverem significativamente fora de sincronia, podem ocorrer erros durante o registro do aplicativo, catalogação de metadados, operações de inventário, tarefas de backup ou tarefas de restauração de arquivos. Para obter mais informações sobre como identificar e resolver o desvio do cronômetro, consulte o artigo da base de conhecimento do VMware a seguir: [Tempo em desvios de máquina virtual devido aos 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 e validado com os seguintes navegadores da web:

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

Se a sua resolução de tela for inferior a 1024 x 768, alguns itens podem não se encaixar na janela. Ative as janelas pop-up no seu navegador para acessar o sistema de ajuda e algumas operações do IBM Spectrum Protect Plus.

Portas de dispositivo virtual

IBM Spectrum Protect Plus e os serviços associados usam as portas a seguir.

Tabela 3. Portas de comunicação quando o destino é um dispositivo virtual IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
22	Transmission Control Protocol (TCP)	servidor vSnap	Dispositivo virtual IBM Spectrum Protect Plus	<p>Fornece acesso para tarefas de resolução de problemas e de manutenção no dispositivo virtual IBM Spectrum Protect Plus usando protocolo SSH.</p> <p>Também usado para replicação de dados vSnap para o dispositivo virtual IBM Spectrum Protect Plus usando protocolo SSH.</p>
443	TCP	IBM Spectrum Protect Plus interface com o usuário	Dispositivo virtual IBM Spectrum Protect Plus	<p>Fornece acesso à web usando HTTPS. Essa porta é o principal ponto de entrada para conexões do cliente que usam protocolo SSL. Essa porta também é usada para consultas Representational State Transfer Application Programming Interface (API REST).</p>
5671	TCP e Advanced Message Queuing Protocol (AMQP)	Host do proxy VMware vStorage API for Data Protection (proxy VADP)	Dispositivo virtual IBM Spectrum Protect Plus	<p>Usado para gerenciar mensagens produzidas e usadas pelos trabalhadores do proxy do VADP e do gerenciamento de tarefa do VMware. Esta porta é uma estrutura de mensagem do RabbitMQ, que também facilita o gerenciamento de log da tarefa.</p>

Tabela 3. Portas de comunicação quando o destino é um dispositivo virtual IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
8090	TCP	Console Administrativo	Dispositivo virtual IBM Spectrum Protect Plus	Fornecer acesso para administração do sistema. Essa estrutura extensível suporta plug-ins que executam operações, como atualizações de sistema e rede.
111	TCP	Hypervisors, proxy VADP ou agentes que usam o cliente do Network File System (NFS)	Dispositivo virtual do IBM Spectrum Protect Plus: servidor vSnap integrado	Permite que clientes Open Network Computing (ONC) descubram portas para comunicação com servidores ONC.
2049	TCP	Hypervisors, proxy do VADP ou agentes que usam o cliente NFS	Dispositivo virtual do IBM Spectrum Protect Plus: servidor vSnap integrado	Usado para transferir compartilhamento de arquivo do NFS pelo servidor vSnap.
3260	TCP	Hypervisors, proxy VADP ou agentes que utilizam o cliente Internet Small Computer System Interface (iSCSI)	Dispositivo virtual do IBM Spectrum Protect Plus: servidor vSnap integrado	Usado para transferência de dados iSCSI pelo servidor vSnap.
20048	TCP	Hypervisors, proxy do VADP ou agentes que usam o cliente NFS	Dispositivo virtual do IBM Spectrum Protect Plus: servidor vSnap integrado	Usado para transferência de dados NFS pelo servidor vSnap.

Atualizações de porta:

- Porta 9090: em versões anteriores, a porta 9090 era usada para ajuda on-line. A partir da versão V10.1.4, essa porta não é mais necessária para ajuda on-line. Nenhuma ação adicional é necessária.
- Porta 8761: em versões anteriores, a porta 8761 era usada para descobrir automaticamente proxies VADP e para operações de backup da máquina virtual (VM) IBM Spectrum Protect Plus. A partir do IBM Spectrum Protect Plus V10.1.6, a arquitetura de proxy VADP foi modificada e a porta 8761 não precisa mais ser aberta. Quando IBM Spectrum Protect Plus é atualizado para V10.1.6, os proxies VADP associados no ambiente também são atualizados.

Tabela 4. Portas de comunicação quando o inicializador é um dispositivo virtual IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
22	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Servidor vSnap ou host do proxy VADP	Fornecer acesso para tarefas de resolução de problemas e de manutenção em servidores vSnap remotos e proxy VADP usando protocolo SSH. Também usado para replicação de dados vSnap a partir do dispositivo virtual IBM Spectrum Protect Plus usando protocolo SSH.
25	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Servidor de e-mail que pode ser acessado usando Protocolo Simples de Transporte de Correio (SMTP)	Fornecer acesso a um serviço de e-mail.
389	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Servidor do protocolo LDAP	Fornecer acesso ao Active Directory Services.
443	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Hypervisor: host VMware Elastic Sky X Integrated (ESXi) e vCenter	Fornecer acesso ao ESXi e ao vCenter para gerenciamento de operações.
636	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Servidor LDAP	Fornecer acesso ao Active Directory Services usando o protocolo SSL.

Tabela 4. Portas de comunicação quando o inicializador é um dispositivo virtual IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
902	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Hypervisor: host do ESXi do VMware	<p>Usado para o protocolo do Network File Copy (NFC), que fornece um serviço do File Transfer Protocol (FTP) ciente de tipo de arquivo para componentes do vSphere.</p> <p>Por padrão, o ESXi usa o NFC para operações, como copiar e mover dados entre os armazenamentos de dados.</p>
5985	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Hypervisor: Hyper-V ou agentes que usam o inicializador iSCSI	Fornece acesso ao serviço do Microsoft Windows Remote Management (WinRM) para servidores baseados no Windows.
5986	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Hypervisor: Hyper-V ou agentes que usam o inicializador iSCSI	Fornece acesso ao serviço do Microsoft Windows Remote Management (WinRM) para servidores baseados no Windows.
8098	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Host do proxy do VADP	Suporta comunicações de API REST entre o dispositivo virtual IBM Spectrum Protect Plus e o proxy VADP usando o protocolo Segurança da Camada de Transporte (TLS).

Tabela 4. Portas de comunicação quando o inicializador é um dispositivo virtual IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
8900	TCP	Dispositivo do IBM Spectrum Protect Plus	servidor vSnap	Suporta comunicações de API de REST entre o dispositivo virtual do IBM Spectrum Protect Plus e o servidor vSnap usando o protocolo do TLS.

Diagrama de caminhos de comunicação do IBM Spectrum Protect Plus

O diagrama a seguir é uma visão geral dos caminhos de comunicação que são gerenciados por IBM Spectrum Protect Plus. Este diagrama pode fornecer assistência para resolução de problemas e configuração de rede para cenários de implementação.

- Os recursos rotulados no plano de fundo cinza representam os serviços principais do dispositivo virtual IBM Spectrum Protect Plus.
- As cores dos vários módulos representam diferentes tipos de serviços, conforme definido pela chave.
- A área que é rotulada como **Firewall** representa o firewall de rede.
- Os serviços que aparecem na área **Firewall** são indicativos das portas que estão abertas no firewall.
- As setas tracejadas representam a comunicação entre recursos e serviços.
- As setas fluem em direção à porta de atendimento.
- Os números de porta que devem estar abertos são indicados pela porta de atendimento.

Por exemplo:

- O serviço vSnap é representado como sendo externo ao dispositivo virtual IBM Spectrum Protect Plus. O serviço vSnap está atendendo na porta 8900 e em outras portas.
- Um componente no dispositivo virtual estabelece um caminho de comunicação com uma conexão com o serviço vSnap na porta 8900.

³ Os agentes a seguir usam um cliente NFS: VMware, Oracle, IBM Db2, MongoDB, Kubernetes e Microsoft Office 365.

⁴ Uma porta SSH conecta o servidor do IBM Spectrum Protect Plus ao agente de suporte de backup do Kubernetes. Se você não selecionar uma porta, um número de porta aleatório será selecionado pelos Serviços NodePort no intervalo padrão. Se você especificar um valor para esta porta, use um número de porta dentro do intervalo NodePort que é configurado pelo administrador do Kubernetes que ainda não está em uso.

Requisitos do servidor vSnap

Instalação 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 quando o dispositivo virtual IBM Spectrum Protect Plus é inicialmente implementado. O servidor vSnap do host local é adequado para fins de demonstração ou de teste. Para uso em um ambiente de produção, é necessário instalar um ou mais servidores vSnap externos.

Aloque memória com base na capacidade de backup para uma deduplicação de dados mais eficiente. Para obter mais informações sobre como construir uma solução IBM Spectrum Protect Plus, consulte [Blueprints do IBM Spectrum Protect Plus](#).

Implementação inicial do servidor vSnap

Para a implementação inicial, assegure-se de que sua VM ou servidor físico Linux® atenda aos seguintes requisitos mínimos:

- – servidor de 8-core 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 em `/opt/vsnap-data`

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

Opcionalmente, use uma unidade de estado sólido (SSD) para ajudar a melhorar o desempenho de backup e restauração:

- Para melhorar o desempenho do backup, configure o conjunto de armazenamentos para usar um ou mais dispositivos de log que são submetidos a backup em 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 de armazenamentos para usar um dispositivo de cache que é submetido a backup em uma SSD.

Instalação da VM do servidor vSnap

Antes de implementar o servidor vSnap para o host, assegure-se de que um dos seguintes requisitos seja atendo:

- 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 níveis de correção (começando com o IBM Spectrum Protect Plus V10.1.2)
- vSphere 7.0, incluindo todas as atualizações e níveis de correção (começando com o IBM Spectrum Protect Plus V10.1.6)
- Microsoft Hyper-V 2016
- Microsoft Hyper-V 2019 (começando com o IBM Spectrum Protect Plus V10.1.3)

Instalação física do servidor vSnap

A partir da versão V10.1.3, IBM Spectrum Protect Plus fornece novas funções que requerem os níveis de kernel que são suportados no Red Hat Enterprise Linux (RHEL) 7.5 e CentOS 7.5. Se você tiver que

usar sistemas operacionais anteriores ao RHEL 7.5 e ao CentOS 7.5, use IBM Spectrum Protect Plus V10.1.2 para instalações físicas do vSnap.

Os seguintes sistemas operacionais Linux são suportados para as instalações do servidor vSnap físico do IBM Spectrum Protect Plus V10.1.6:

- CentOS 7.1804 (7.5) (x86_64) (começando com IBM Spectrum Protect Plus V10.1.2)
- CentOS 7.1810 (7.6) (x86_64) (começando com IBM Spectrum Protect Plus V10.1.3 patch 1)
- CentOS 7.1908 (7.7) (x86_64) (começando com IBM Spectrum Protect Plus V10.1.5 patch 1)
- RHEL 7.5 (x86_64) (começando com IBM Spectrum Protect Plus V10.1.2)
- RHEL 7.6 (x86_64) (começando com IBM Spectrum Protect Plus V10.1.3 patch1)
- RHEL 7.7 (x86_64) (começando com IBM Spectrum Protect Plus V10.1.5 patch1)

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

- CentOS 7.3.1611 (x86_64)
- CentOS 7.4.1708 (x86_64)
- RHEL 7.3 (x86_64)
- RHEL 7.4 (x86_64)

portas do servidor vSnap

As portas a seguir são usadas por servidores vSnap.

Tabela 5. Portas de comunicação quando o destino é um servidor vSnap				
Porta	Protocolo	Iniciador	Resposta	Descrição
22	TCP	Dispositivo virtual, hypervisors ou agentes do IBM Spectrum Protect Plus que usam o cliente NFS	servidor vSnap	Fornece acesso para tarefas de resolução de problemas e de manutenção em servidores vSnap usando protocolo SSH.
111	TCP	Hypervisors, proxy do VADP ou agentes que usam o cliente NFS	servidor vSnap	Permite que os clientes do ONC descubram portas para comunicação com servidores ONC.
445	TCP	Agentes de aplicativos que utilizam o Bloco de Mensagens do Servidor (SMB) ou o protocolo Common Internet File System (CIFS)	servidor vSnap	Fornece uma porta de destino que é usada pelo servidor vSnap por meio do protocolo SMB ou CIFS para montar compartilhamentos do sistema de arquivos para operações de backup e recuperação de log de transações.

Tabela 5. Portas de comunicação quando o destino é um servidor vSnap (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
2049	TCP	Hypervisors, proxy do VADP ou agentes que usam o cliente NFS	servidor vSnap	Usado para compartilhamento de arquivos NFS pelo servidor vSnap.
3260	TCP	Hypervisors, proxy VADP ou agentes que usam o cliente iSCSI	servidor vSnap	Usado para transferência de dados iSCSI por servidores vSnap.
8900	TCP	Dispositivo virtual IBM Spectrum Protect Plus	servidor vSnap	Suporta comunicações de API de REST entre o dispositivo virtual do IBM Spectrum Protect Plus e o servidor vSnap usando o protocolo do TLS.
20048	TCP	Hypervisors, proxy do VADP ou agentes que usam o cliente NFS	servidor vSnap	Monta sistemas de arquivos vSnap em clientes, como o proxy VADP, servidores de aplicativos e armazenamentos de dados de virtualização. Essa porta também é usada para transferência de dados do NFS para servidores vSnap.

Informações importantes de segurança: processe solicitações para portas de dados vSnap (NFS, SMB e iSCSI) somente quando a solicitação vier de um nó na rede interna. As solicitações que vêm de nós da rede externa (não privada) devem ser bloqueadas. Para garantir que as práticas de segurança adequadas sejam seguidas, trabalhe com o administrador de segurança de rede.

Atualização de portas: em versões anteriores, as portas 137, 138 e 139 no servidor vSnap foram usadas por agentes de aplicativo que usam SMBv1. Iniciando com o IBM Spectrum Protect Plus V10.1.6, o protocolo do SMBv1 não é usado. Todos os agentes usam o SMBv2 ou mais recente, que não requer as portas 137, 138 ou 139.

Requisitos do proxy do VADP

Instalação do proxy VADP

Em IBM Spectrum Protect Plus, executar tarefas de backup de VM através do VADP requer recursos significativos do sistema. Ao criar proxies de tarefa de backup do VADP, você ativa o compartilhamento de carregamento e o balanceamento de carga para as tarefas de backup do IIBM Spectrum Protect Plus. Se os proxies existirem, toda a carga de processamento será deslocada do dispositivo virtual IBM Spectrum Protect Plus para os proxies.

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

Este recurso é suportado apenas em quad core de 64 bits ou configurações superiores com uma versão de kernel mínima de v2.6.32 nos seguintes ambientes do Linux:

- Níveis de manutenção e de modificação do CentOS 6.5 e mais recentes (começando com IBM Spectrum Protect Plus V10.1.1 patch 1)
- Níveis de manutenção e de modificação do CentOS 7.0 e mais recentes (começando com IBM Spectrum Protect Plus V10.1.1 patch 1)
- Níveis de manutenção e de modificação do RHEL 6.4 e mais recentes (começando com IBM Spectrum Protect Plus V10.1.1)
- Níveis de manutenção e de modificação do RHEL 7 e mais recentes (começando com IBM Spectrum Protect Plus V10.1.1)
- Níveis de manutenção e de modificação do SUSE Linux Enterprise Server (SLES) 12 e mais recentes (começando com IBM Spectrum Protect Plus V10.1.1)

Para obter mais informações sobre como construir uma solução IBM Spectrum Protect Plus, consulte o [Blueprints do IBM Spectrum Protect Plus](#)

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

- Processador quad core de 64 bits
- 8 GB de memória de acesso aleatório (RAM) necessários, 16 GB preferencial
- 60 GB de espaço livre em disco

Devido ao aumento do uso do processador e da simultaneidade no servidor proxy VADP, a memória que está alocada no servidor proxy deve ser aumentada.

O proxy deve ser capaz de montar sistemas de arquivos NFS, que, em muitos casos, requerem que um pacote de clientes NFS seja instalado. Os detalhes 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 alcançáveis a partir do proxy.

A porta 8098 no servidor proxy VADP deve ser aberta quando o firewall do servidor proxy está ativado.

Para criar proxies VADP, deve-se ter um ID do usuário com a função SYSADMIN atribuída. Para obter mais informações sobre funções, consulte [“Gerenciando atribuições”](#) na página 521.

Portas de proxy do VADP

As seguintes portas são usadas por proxies VADP.

Tabela 6. Portas de comunicação quando o destino é um host do proxy VADP				
Porta	Protocolo	Iniciador	Resposta	Descrição
22	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Host do proxy do VADP	Fornecer acesso para tarefas de resolução de problemas e de manutenção em hosts do proxy VADP usando o protocolo SSH.

Tabela 6. Portas de comunicação quando o destino é um host do proxy VADP (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
8098	TCP	Dispositivo virtual IBM Spectrum Protect Plus	Host do proxy do VADP	Suporta comunicações de API REST entre o dispositivo virtual IBM Spectrum Protect Plus e o proxy VADP usando o protocolo TLS.

Tabela 7. Portas de comunicação quando o iniciador é um host do proxy VADP

Porta	Protocolo	Iniciador	Resposta	Descrição
111	TCP	Host do proxy do VADP	servidor vSnap	Permite que os clientes do ONC descubram portas para comunicação com servidores ONC.
443	TCP	Host do proxy do VADP	Hypervisor: host do VMware ESXi e vCenter	Fornece acesso ao ESXi e ao vCenter para gerenciamento de operações.
902	TCP	Host do proxy do VADP	Hypervisor: host do ESXi do VMware	Usado para o protocolo do Network File Copy (NFC), que fornece um serviço do File Transfer Protocol (FTP) cliente 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.
2049	TCP	Host do proxy do VADP	servidor vSnap	Usado para transferir compartilhamento de arquivo do NFS pelo servidor vSnap.

Tabela 7. Portas de comunicação quando o iniciador é um host do proxy VADP (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
5671	TCP e AMQP	Host do proxy do VADP	Dispositivo virtual IBM Spectrum Protect Plus	Usado para gerenciar mensagens produzidas e usadas pelos trabalhadores do proxy do VADP e do gerenciamento de tarefa do VMware. Esta porta é uma estrutura de mensagem do RabbitMQ, que também facilita o gerenciamento de log da tarefa.
20048	TCP	Host do proxy do VADP	servidor vSnap	Monta sistemas de arquivos vSnap em clientes, como o proxy VADP, servidores de aplicativos e armazenamentos de dados de virtualização. Essa porta também é usada para transferência de dados do NFS para servidores vSnap.

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

Atualizações de portas: em versões anteriores, a porta 8761 foi usada para descobrir automaticamente proxies VADP e para operações de backup de máquina virtual (VM) IBM Spectrum Protect Plus. A partir do IBM Spectrum Protect Plus V10.1.6n, a arquitetura de proxy VADP foi modificada e a porta 8761 não precisa mais ser aberta. Quando IBM Spectrum Protect Plus é atualizado para a versão V10.1.6, os proxies VADP associados no ambiente também são atualizados.

Se o script de comando do firewall não estiver disponível em seu sistema, edite o firewall manualmente para abrir ou fechar as portas necessárias e reinicie o firewall. Para obter instruções sobre a edição de portas de firewall, consulte [“Editando portas de firewall”](#) na página 104.

Proxy VADP no servidor vSnap

Os proxies VADP podem ser instalados nos servidores vSnap em seu ambiente do IBM Spectrum Protect Plus. Uma combinação de proxy VADP e servidor vSnap deve atender aos requisitos mínimos de ambos os dispositivos. Considere os requisitos do sistema de ambos os dispositivos e inclua os requisitos de core e RAM juntos para identificar os requisitos mínimos da combinação de proxy VADP e servidor vSnap.

Para um proxy VADP instalado em um servidor vSnap virtual, os requisitos a seguir devem ser atendidos:

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

Todos os “[Portas de proxy do VADP](#)” na página 34 e “[portas do servidor vSnap](#)” na página 32 necessários devem estar abertos na combinação de proxy VADP e servidor vSnap.

Requisitos de Conectividade

- O IBM Spectrum Protect Pluss usa o Network File System (NFS) para montar volumes de armazenamento para operações de backup e restauração. No Linux, assegure-se de que o cliente NFS do Linux nativo esteja instalado.
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus podem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles deverão ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e por meio do servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.
- Se o DNS não estiver disponível, você deverá incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual do IBM Spectrum Protect Plus usando a linha de comandos.

Requisitos de armazenamento do servidor do repositório

Se você planeja usar o IBM Spectrum Protect como um servidor de repositório para copiar dados para armazenamento em nuvem, assegure-se de que esteja usando IBM Spectrum Protect V8.1.10.

Requisitos de armazenamento em nuvem

Área de cache de disco

Para todas as funções relacionadas às operações de cópia e restauração de dados para e de destinos de nuvem e arquivamento, o servidor vSnap requer que uma área de cache de disco esteja presente no servidor vSnap:

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

Para obter instruções sobre dimensionamento e instalação do cache, consulte o [Blueprints do IBM Spectrum Protect Plus](#).

Caminhos múltiplos

Durante as operações de cópia para o armazenamento de objetos, o IBM Spectrum Protect Plus conecta e remove dispositivos de nuvem virtual em servidores vSnap. Se a configuração de caminhos múltiplos for ativada no servidor vSnap usando **dm-multipath**, a configuração poderá interferir na operação de cópia. Para evitar essa interferência, os dispositivos de nuvem virtual devem ser excluídos da configuração de caminhos múltiplos. Inclua as linhas a seguir na seção de lista de bloqueio do arquivo de configuração de caminhos múltiplos `/etc/multipath.conf`:

```
blacklist {
    device {
        vendor "LIO-ORG"
        product ".*"
    }
}
```

Depois de fazer essa alteração, recarregue a configuração de caminhos múltiplos usando o seguinte comando:

```
sudo systemctl reload multipathd
```

Certificados

- **Certificados autoassinados:** se o terminal de nuvem ou servidor de repositório usar um certificado autoassinado, você deverá especificar o certificado no formato Privacy Enhanced Mail (PEM) quando registrar a nuvem ou o servidor do repositório na interface com o usuário do IBM Spectrum Protect Plus.
- **Certificados assinados por Autoridade de Certificação privada:** se o terminal de nuvem ou 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 o servidor em nuvem ou repositório na interface com o usuário do IBM Spectrum Protect Plus. Além disso, deve-se incluir o certificado raiz ou intermediário da CA privada 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 por Autoridade de Certificação pública:** se o terminal em nuvem utilizar 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.

Rede

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

Tabela 8. Portas de comunicação quando o destino é um servidor de nuvem ou terminal do servidor de repositório				
Porta	Protocolo	Iniciador	Resposta	Descrição
443	TCP	servidor vSnap	Terminais do servidor em nuvem	Permite que o servidor vSnap se comunique com os terminais do Amazon Simple Storage Service (S3), Microsoft Azure ou IBM Cloud Object Storage.
9000	TCP	servidor vSnap	Terminais do servidor de repositório	Permite que o servidor vSnap se comunique com os terminais do IBM Spectrum Protect (servidor de repositório).

Quaisquer firewalls ou proxies de rede que inspecionam SSL ou conduzem uma inspeção abrangente de pacote de tráfego entre os servidores vSnap e terminais de nuvem podem interferir na validação do certificado SSL em servidores vSnap. Essa interferência também pode causar falhas na tarefa de

cópia em nuvem. Para evitar essa interferência, os servidores vSnap devem ser isentos da interceptação de SSL e da inspeção na configuração de firewall ou de proxy.

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 contínua na qual 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 leva à distorção de dados.

Se o provedor de nuvem usar um certificado SSL que é autoassinado ou assinado por uma autoridade de certificação privada, consulte [Requisitos do certificado](#).

• Requisitos de nuvem do Amazon S3

- **Armazenamento de objeto padrão:** 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.
- **Armazenamento de objeto de archive:** quando o provedor em nuvem é registrado em 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. IBM Spectrum Protect Plus faz diretamente o upload de arquivos de dados para a camada do Glacier. Alguns arquivos de metadados pequenos são 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

- **Armazenamento de objeto padrão:** quando o provedor em nuvem é registrado em IBM Spectrum Protect Plus, um depósito existente deve ser especificado. Se o depósito especificado tiver uma política Write Once Read Many (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 depósito deve ter a configuração Name Index ativada.
- **Armazenamento de objeto de archive:** quando o provedor de 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. O depósito deve ter a configuração Name Index ativada.

• Requisitos do Microsoft Azure

- **Armazenamento de objeto padrão:** 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.
- **Armazenamento de objeto de 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 são movidos imediatamente para a camada de archive e retornados temporariamente para a camada quente apenas durante as operações de restauração. Alguns arquivos de metadados pequenos são 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)

- **Armazenamento de objeto padrão:** 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.

- **Armazenamento de objeto de 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. IBM Spectrum Protect Plus faz diretamente o upload de arquivos de dados para o armazenamento de fita do IBM Spectrum Protect. Alguns arquivos de metadados pequenos são armazenados no armazenamento de objeto 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.

<i>Tabela 9. Requisitos de cópia e cópia de archive para provedores em nuvem</i>		
Operação	Provedor	Requisitos
Cópia	Amazon S3	Um depósito existente deve ser especificado a partir de uma das camadas de armazenamento suportadas.
Cópia	IBM Cloud Object Storage	Um depósito existente deve ser especificado. O depósito deve ter a configuração Name Index ativada.
Cópia	Microsoft Azure	Um contêiner existente deve ser especificado a partir de uma camada de armazenamento quente ou frio.
Cópia	IBM Spectrum Protect	O IBM Spectrum Protect Plus cria seu próprio depósito exclusivo.
Cópia arquivada	Amazon S3	O servidor vSnap deve ser capaz de se comunicar com os terminais do IBM Spectrum Protect (servidor de repositório).
Cópia arquivada	IBM Cloud Object Storage	Um depósito existente deve ser especificado a partir da camada de archive. O depósito deve ter a configuração Name Index ativada.
Cópia arquivada	Microsoft Azure	Um contêiner existente deve ser especificado a partir da camada de armazenamento quente e da camada de archive.
Cópia arquivada	IBM Spectrum Protect	O IBM Spectrum Protect Plus cria seu próprio depósito exclusivo para ser copiado para a fita IBM Spectrum Protect.

Requisitos de restauração e backup do hypervisor (Microsoft Hyper-V e VMware) e da instância da nuvem (Amazon EC2)

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 [Nota técnica 304861](#).

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
- Hyper-V Server 2019 (a partir do IBM Spectrum Protect Plus V10.1.4) ou Microsoft Hyper-V no Windows Server 2019 (a partir do IBM Spectrum Protect Plus V10.1.3)

IBM Spectrum Protect Plus protege as máquinas virtuais (VMs) que estão habilitadas para usar o recurso Hyper-V Replica. Dependendo do seu ambiente Hyper-V, você pode ser obrigado a atualizar algumas políticas de acordo de nível de serviço (SLA) ao atualizar o ambiente do seu sistema para IBM Spectrum Protect Plus V10.1.6. Para obter mais informações sobre os requisitos para atualização de VMs em ambientes Hyper-V, [“Etapas adicionais para atualização de máquinas virtuais em ambientes de Réplica do Hyper-V” na página 180](#),

Para proteger os dados do Hyper-V, primeiro inclua os servidores Hyper-V em IBM Spectrum Protect Plus e, em seguida, crie tarefas para fazer backup e restaurar os dados do Hyper-V, conforme descrito em [“Fazendo Backup e Restaurando Dados do Hyper-V” na página 275](#).

Antes de configurar servidores Hyper-V, revise os requisitos para cada etapa de configuração:

- Registrando os provedores dos quais você deseja fazer backup.

Os servidores Hyper-V podem ser registrados usando um nome de DNS (Domain Name System) ou um endereço IP (Protocolo de Internet). 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 do cluster deverão ser resolvíveis pelo DNS. Se o DNS não estiver disponível, você deverá incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual do 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.

- Configurando políticas de SLA.

Se uma VM estiver associada a múltiplas políticas de SLA, assegure-se de que as políticas não estejam planejadas para serem executadas 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 VM for protegida por uma política de SLA, os backups da VM serão retidos com base nos parâmetros de retenção da política de SLA, mesmo que a VM seja removida.

- Garantindo que os mais novos serviços de integração do Hyper-V estejam instalados:
 - Para ambientes Microsoft Windows, consulte [Sistemas operacionais guest Windows suportados para o Hyper-V no Windows Server](#)
 - Para ambientes Linux®, consulte [Máquinas virtuais suportadas Linux e FreeBSD para Hyper-V em Windows](#)

Antes de fazer backup ou restaurar dados do Hyper-V, execute as ações a seguir:

- Certifique-se de que o Serviço Inicializador iSCSI do Microsoft esteja em execução em todos os servidores do Hyper-V, incluindo nós de cluster. Na janela Serviços, configure o tipo de inicialização para o Serviço Inicializador iSCSI da Microsoft como **Automático** para que o serviço esteja disponível quando o servidor Hyper-V ou 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.

- Assegure-se de que as funções e os grupos de recursos apropriados sejam atribuídos aos usuários que iniciarão as operações de backup e restauração. Conceda aos usuários acesso a funções e grupos de recursos usando a área de janela de Contas. Inclua o usuário no grupo de administradores locais no servidor Hyper-V.

- Se você pretende restaurar uma VM usando o modo de clone e usando a configuração IP original, assegure-se de que as credenciais sejam estabelecidas por meio das opções Nome do Usuário do OS Guest e Senha do OS Guest dentro da definição de tarefa de backup.

Restrições

- Para dados do Hyper-V, as operações de backup e restauração são suportadas apenas para discos rígidos virtuais (VHDX). Para obter mais informações, consulte [Problemas Conhecidos e Limitações: IBM Spectrum Protect Plus V10.1.6.x](#)
- Ao restaurar arquivos de um archive IBM Spectrum Protect, os arquivos são migrados inicialmente do armazenamento em fita para um conjunto temporário. Dependendo do tamanho dos arquivos para restauração, esse processo pode levar várias horas.

Requisitos do VMware

As seguintes versões do VMware vSphere são suportadas:

- 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 níveis de correção (começando com o IBM Spectrum Protect Plus V10.1.2)
- vSphere 7.0, incluindo todas as atualizações e níveis de correção (começando com o IBM Spectrum Protect Plus V10.1.6)

Assegure-se de que a versão mais recente do VMware Tools esteja instalada em VMs do VMware.

IBM Spectrum Protect Plus suporta tags de VM VMware.

O backup e a restauração da VM criptografada são suportados com o vSphere 6.5 e posterior.

Um volume de Network File System (NFS) pode ser montado em qualquer número de data centers que pertencem ao mesmo vCenter. Se um volume do NFS estiver montado em mais de um data center, o vCenter tratará o mesmo volume como dois armazenamentos de dados diferentes. O IBM Spectrum Protect Plus o trata como um único armazenamento de dados e combina todas as VMs e discos de máquina virtual (VMDKs) residindo no armazenamento de dados de todos os data centers em que o armazenamento de dados está montado. Qualquer seleção de SLA com relação a esse armazenamento de dados faz com que todas as VMs dos diferentes data centers sejam submetidas a backup ou restauradas no IBM Spectrum Protect Plus.

IBM Spectrum Protect Plus V10.1.5 e posterior protege VMs que são gerenciadas por um VMware Cloud (VMC) em um Software-Defined Data Center (SDDC) do Amazon Web Services (AWS). Para obter mais informações, consulte [IBM Spectrum Protect Plus for VMware Cloud on AWS](#)

Para proteger os dados do VMware, primeiro inclua as instâncias do vCenter Server no IBM Spectrum Protect Plus e, em seguida, crie tarefas para fazer backup e restaurar dados, conforme descrito em [“Fazendo Backup e Restaurando Dados do VMware”](#) na página 249.

- Quando uma instância do vCenter Server é incluída em IBM Spectrum Protect Plus, um inventário da instância é capturado. O inventário é necessário para que os usuários possam concluir tarefas de backup e restauração e executar relatórios.
- Pelo menos uma política de SLA deve ser configurada para os dados do VMware.
- 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 funções e grupos de recursos usando a área de janela de Contas.
- Se uma VM estiver associada a múltiplas políticas de SLA, assegure-se de que as políticas não estejam planejadas para serem executadas 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.

- Assegure-se de que os destinos para tarefas de restauração sejam registrados em IBM Spectrum Protect Plus. Esse requisito se aplica a tarefas de restauração que restauram dados para novos hosts ou clusters.
- Se você pretende restaurar uma VM usando o modo de clone e usando a configuração IP original, assegure-se de que as credenciais sejam estabelecidas por meio das opções Nome do Usuário do OS Guest e Senha do OS Guest dentro da definição de tarefa de backup.

Restrições

- Os modelos de VM restaurados não podem ser ligados após a recuperação de uma VM.
- As chaves de Shell Seguro (SSH) não são um mecanismo de autorização válido para as plataformas Windows.
- Assegure-se de que a versão mais recente do VMware Tools esteja instalada em seu ambiente.
- Os volumes Physical RDM (pRDM) não suportam capturas instantâneas. VMs que contêm um ou mais volumes de raw device-mapping (RDM) fornecidos no modo pRDM são submetidas a backup. No entanto, os volumes pRDM não são processados como parte da operação de backup da VM.

Requisitos do Amazon EC2

A partir do IBM Spectrum Protect Plus Versão V10.1.6, o suporte é incluído ou faz backup e restaura dados em instâncias do Amazon EC2.

Para proteger os dados do Amazon EC2, primeiro inclua uma conta EC2 no IBM Spectrum Protect Plus e, em seguida, crie tarefas para operações de backup e restauração para as instâncias EC2 que estão associadas a essa conta, conforme descrito em [“Fazendo backup e restaurando dados do Amazon EC2” na página 288](#).

Antes de fazer backup ou restaurar dados do Amazon EC2, revise os seguintes requisitos:

- Para incluir uma conta EC2 em IBM Spectrum Protect Plus, as chaves de acesso são necessárias. As chaves de acesso são credenciais de longo prazo para um usuário do gerenciamento de acesso e de identidade (IAM) ou o usuário raiz da conta AWS.
- Quando uma conta do Amazon EC2 é incluída no IBM Spectrum Protect Plus, um inventário das instâncias que estão associadas à conta é capturado. Em seguida, é possível executar tarefas de backup e de restauração e gerar relatórios para as instâncias.
- Assegure-se de que uma ou mais políticas de SLA estejam configuradas para as instâncias do EC2.
- Assegure-se de que funções e grupos de recursos do IBM Spectrum Protect Plus sejam designados ao usuário que irá configurar tarefas de backup e restauração.
- Se uma conta estiver associada a múltiplas políticas de SLA, assegure-se de que as políticas não estejam planejadas para serem executadas 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.
- Assegure-se de que os destinos que você pretende usar para tarefas de restauração sejam registrados no IBM Spectrum Protect Plus.

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 [Nota técnica 304861](#).

Geral

- Para operações do hypervisor, o IBM Spectrum Protect Plus suporta apenas os sistemas operacionais que estão disponíveis para seus hypervisors. Para obter informações sobre sistemas operacionais suportados, revise a documentação do hypervisor.

- O IBM Spectrum Protect Plus pode proteger e restaurar máquinas virtuais (VMs) com sistemas de arquivos que não estão listados nesta documentação, mas somente os sistemas de arquivos listados são elegíveis para operações de indexação e restauração de arquivo.
- Os discos de Internet Small Computer Interface (iSCSI) que são mapeados diretamente para o sistema operacional guest não serão indexados. Os volumes suportados incluem volumes de disco da máquina virtual (VMDK) que são montados conforme especificado pela configuração da VM associada.
- A quantidade de espaço livre que é necessária para os metadados no catálogo depende do número total de arquivos no ambiente. Para catalogar 1 milhão de arquivos, o volume do catálogo no dispositivo virtual IBM Spectrum Protect Plus requer aproximadamente 350 MB de espaço livre por versão retida. O espaço que é usado por metadados de indexação de arquivos é recuperado quando as instâncias de backup correspondentes expiram.
- A indexação de arquivo e a restauração de arquivo não são suportadas por meio dos pontos de restauração que foram copiados para recursos em nuvem ou servidores do repositório.
- Um arquivo pode ser restaurado para um local alternativo apenas se as credenciais foram estabelecidas para a máquina virtual alternativa através da opção **Nome do Usuário do OS Guest** e **Senha do OS Guest** na definição de tarefa de backup.

Requisitos do VMware

- Assegure-se de que a versão mais recente do VMware Tools esteja instalada em VMs do VMware.
- Nas configurações da VM em Configuração Avançada, o parâmetro **disk.EnableUUID** deve ser configurado como `true`.

requisitos do Hyper-V

- Assegure-se de que a versão mais recente Hyper-V Integration Services esteja instalada em suas VMs do Hyper-V.
- As operações de indexação e restauração de arquivo suportam discos Small Computer System Interface (SCSI) em um ambiente Hyper-V:
 - Apenas volumes em discos SCSI são elegíveis para a catalogação de arquivos e restauração de arquivo.
 - Discos Integrated Drive Electronics (IDE) não são suportados.

Requisitos do Windows










Tabela 10. Matriz de cobertura para sistemas operacionais suportados no Windows x64				
IBM Spectrum Protect Plus	Windows Server 2008 R2* Edições padrão e de data center	Windows Server 2012 R2 e Windows Server 2012R2 core* Edições padrão e de data center	Windows Server 2016 e Windows Server 2016 core* Edições padrão e de data center	Windows Server 2019 e Windows Server 2019 core* Edições padrão e de data center
V10.1.0				--
V10.1.1				--
V10.1.2				--

Tabela 10. Matriz de cobertura para sistemas operacionais suportados no Windows x64 (continuação)

IBM Spectrum Protect Plus	Windows Server 2008 R2* Edições padrão e de data center	Windows Server 2012 R2 e Windows Server 2012R2 core* Edições padrão e de data center	Windows Server 2016 e Windows Server 2016 core* Edições padrão e de data center	Windows Server 2019 e Windows Server 2019 core* Edições padrão e de data center
V10.1.3	✓	✓	✓	✓ (Apenas Windows Server 2019 core)
V10.1.4	✓	✓	✓	✓
V10.1.5	✓	✓	✓	✓
V10.1.6	✓	✓	✓	✓

* A liberação base e os níveis de manutenção posteriores são suportados.

Tabela 11. Matriz de cobertura para sistemas de arquivos e tipos de armazenamento em disco suportados

Sistemas de Arquivos Suportados	<ul style="list-style-type: none"> • New Technology File System (NTFS) • Resilient File System (ReFS) • Tabela de alocação de arquivo (FAT)
Tipos de armazenamento em disco suportados	<p>Discos básicos com as seguintes partições:</p> <ul style="list-style-type: none"> • MBR (Master Boot Record) • GPT (GUID Partition Table) <p>Restrição: não é possível fazer backup ou restaurar arquivos em discos dinâmicos.</p>

Restrições

- O Windows Remote Shell (WinRM) deve estar ativado.
- **Importante:** IBM Spectrum Protect Plus pode proteger e restaurar VMs com sistemas de arquivos que não estão listados neste documento, mas somente os sistemas de arquivos listados são elegíveis para indexação e restauração de arquivo.
- Quando os arquivos são indexados em um ambiente Windows, os diretórios a seguir no recurso são ignorados:

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

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

- A indexação de arquivo e a restauração de arquivo de uma VM Windows requerem que o caminho binário do Windows PowerShell esteja configurado na variável de ambiente %PATH%.

- Os sistemas de arquivos criptografados Windows não são suportados para catalogação de arquivo ou restauração de arquivo.
- Ao restaurar arquivos em um ambiente do Resilient File System (ReFS), a restauração de tarefas de versões mais recentes do Windows Server para versões anteriores não é suportada. Por exemplo, não é possível restaurar um arquivo do Windows Server 2016 para o Windows Server 2012.
- A catalogação de arquivos, o backup, as restaurações point-in-time e outras operações que invocam o agente Windows falharão se um administrador local não padrão for inserido como o Nome do Usuário do OS 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 for configurado como 0 ou não for configurado, um administrador local não padrão não poderá interagir com o WinRM, que é o protocolo que o IBM Spectrum Protect Plus utiliza para instalar o agente Windows para catalogação de arquivo, enviar comandos para esse agente e obter resultados dele.

Configure a chave de registro do LocalAccountTokenFilterPolicy para a versão 1 no guest Windows que está sendo submetido a backup com o Catalog File Metadata ativado. 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.

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 são excluídos quando a indexação é concluída. A quantia de espaço livre necessária para os metadados depende do número total de arquivos no sistema. Assegure-se de que aproximadamente 350 MB de espaço livre esteja disponível por um milhão de arquivos.

Requisitos de Conectividade

- O nome do host do dispositivo virtual IBM Spectrum Protect Plus deve ser resolvível a partir da VM Windows.
- O endereço IP (Internet Protocol) da VM que é selecionado para indexação deve estar visível para o cliente vSphere ou o Hyper-V Manager.
- A VM Windows que é selecionada para indexação deve suportar conexões de saída para a porta 22, que usa o protocolo Secure Shell (SSH), no dispositivo virtual IBM Spectrum Protect Plus.
- O serviço do Microsoft Windows Remote Management (WinRM) deve estar em execução.
- Os firewalls devem ser configurados para ativar o IBM Spectrum Protect Plus para se conectar ao servidor usando o WinRM.
- O endereço IP da máquina que você registra deve ser acessível por meio do servidor IBM Spectrum Protect Plus e por meio do servidor vSnap. Ambos os servidores devem ter um serviço WinRM atendendo na porta 5985.
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus podem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles deverão ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e por meio do servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.

Requisitos de autenticação e de privilégio

As credenciais que são especificadas para uma VM devem incluir um usuário com os seguintes privilégios:

- A identidade do usuário deve ter o direito **Efetuar Logon como um Serviço**, que é designado através do painel de controle Ferramentas Administrativas no servidor 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 usa o protocolo Windows Challenge/Response (NTLM) e a identidade do usuário segue o formato padrão domain\Name se a VM do Hyper-V estiver conectada a um domínio. O formato local administrator será usado se o usuário for um administrador local. As credenciais devem ser estabelecidas para a VM associada usando a opção **Nome do Usuário do OS Guest e Senha do OS Guest** dentro da definição de tarefa de backup associada.
- As credenciais de login do sistema devem ter as permissões do administrador local.

Requisitos do Kerberos

- A autenticação baseada em Kerberos pode ser ativada por meio de um arquivo de configuração no dispositivo virtual IBM Spectrum Protect Plus. Essa configuração substitui o protocolo NTLM do Windows padrão. O Kerberos não suporta o uso de contas de usuários locais e é adequado apenas para ambientes em que todas as VMs estão em um único domínio.
- Somente para autenticação baseada em Kerberos, a identidade do usuário deve ser especificada no formato username@FQDN. O usuário especificado 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 que é especificado pelo nome completo do domínio.
- A autenticação do Kerberos também requer que o clock skew entre o controlador de domínio e o dispositivo virtual IBM Spectrum Protect Plus seja menor que 5 minutos. O protocolo NTLM padrão do Windows não é dependente de tempo.

Requisitos do Objeto de Política de Grupo

É possível especificar a configuração de Objeto de política de grupo (GPO) navegando para:

- **Configuração do computador > Políticas > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança > Segurança de rede: NTLM restrito: tráfego de NTLM recebido**

Ou este

- **Configuração do computador > Políticas > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança > Segurança de rede: NTLM restrito: tráfego de NTLM de saída**

Em seguida, escolha uma das opções a seguir:

- **Permitir Tudo**
- **Permitir todas as contas**

Requisitos do Linux











Tabela 12. Matriz de cobertura para sistemas operacionais suportados no Linux® x86_64								
IBM Spectrum Protect Plus	RHEL 6.4*	RHEL 7.0*	RHEL 8.0*	CentOS 6.4*	CentOS 7.0*	CentOS 8.0*	SLES 12.0*	SLES 15.0*
V10.1.0			--			--		--
V10.1.1			--			--		--

Tabela 12. Matriz de cobertura para sistemas operacionais suportados no Linux® x86_64 (continuação)

IBM Spectrum Protect Plus	RHEL 6.4*	RHEL 7.0*	RHEL 8.0*	CentOS 6.4*	CentOS 7.0*	CentOS 8.0*	SLES 12.0*	SLES 15.0*
V10.1.2	✓	✓	--	✓	✓	--	✓	--
V10.1.3	✓	✓	--	✓	✓	--	✓	--
V10.1.4	✓	✓	--	✓	✓	--	✓	--
V10.1.5	✓	✓	--	✓	✓	--	✓	--
V10.1.6	✓	✓	✓	✓	✓	✓	✓	✓

* A liberação base e os níveis de manutenção posteriores são suportados.

Tabela 13. Matriz de cobertura para sistemas de arquivos suportados

Sistemas de Arquivos Suportados	<ul style="list-style-type: none"> • ext2 • ext3 • ext4 • XFS
--	---

Restrições

- Um sistema de arquivos que foi criado em uma versão do kernel mais recente pode não ser montável em um sistema com uma versão do kernel anterior. Nesse caso, a restauração de arquivos do sistema mais novo para o anterior não é suportada.
- Quando os arquivos são indexados 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 são então excluídos quando a indexação é concluída. A quantia de espaço livre necessária para os metadados depende do número total de arquivos no sistema. Assegure-se de que aproximadamente 350 MB de espaço livre esteja disponível por um milhão de arquivos.

Requisitos de software

- Os pacotes **bash** e **sudo** devem ser instalados. O pacote **sudo** deve estar na versão 1.7.6p2 ou posterior. Execute **sudo -V** para verificar a versão.

Dica: Os pacotes **bash** **necessário** e **sudo** necessários estão incluídos nos sistemas operacionais Linux 86_64 suportados.

- Certifique-se de que a versão suportada do Linux x86_64 esteja instalada.
- O International Components for Unicode (libicu) rpm-pacote que corresponde ao sistema operacional deve ser instalado.
- Em um ambiente Linux, assegure-se de que o pacote do utilitário Linux, **util-linux-ng**, ou o pacote **util-linux** seja atual.
- Assegure-se de que o valor **ulimit -f** do tamanho do arquivo efetivo para o usuário do agente IBM Spectrum Protect Plus e o usuário da instância do IBM Db2 esteja configurado como **unlimited**. Como alternativa, configure o valor para um valor suficientemente alto para permitir a cópia dos arquivos maiores de banco de dados em suas tarefas de backup e de restauração. Se você alterar a configuração **ulimit**, reinicie a instância do Db2 para finalizar a configuração.
- **Usuários do Red Hat® Enterprise Linux e CentOS 6:**

Assegure-se de que o pacote **util-linux-ng** seja atual executando o seguinte comando:

```
yum update util-linux-ng
```

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

- Se os dados residirem em volumes LVM (Gerenciador de Volume Lógico), assegure-se de que a versão do LVM seja 2.0.2.118 ou mais recente.

Execute o comando **lvm version** para verificar a versão e execute o comando **yum update lvm2** para atualizar o pacote, se necessário.

- Se os dados residirem em volumes do LVM, o serviço **lvm2-lvmetad** deverá ser desativado, pois pode interferir na capacidade do IBM Spectrum Protect Plus de montar e renunciar às capturas instantâneas e 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 arquivo **/etc/lvm/lvm.conf** e especifique a configuração a seguir:

```
use_lvmetad = 0
```

Para obter mais informações, consulte [O Daemon de Metadados \(lvmetad\)](#).

- Se os dados residirem em sistemas de arquivos XFS e a versão do pacote **xfsprogs** ficar entre 3.2.0 e 4.1.9, a operação de restauração de arquivo pode falhar devido a um problema conhecido no **xfsprogs**, que causa a distorção de um sistema de arquivos de clone ou captura instantânea quando o identificador exclusivo universal (UUID) é modificado. Para resolver esse problema, atualize o **xfsprogs** para a versão 4.2.0 ou posterior. Para obter mais informações, consulte [Logs de relatório Debian Bug](#)

Requisitos de Conectividade

- O subsistema Secure File Transfer Protocol (SFTP) para SSH está ativado.
- O serviço SSH está em execução na porta 22 no servidor host do proxy.
- Os firewalls são configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor host do proxy usando o SSH.
- O IBM Spectrum Protect Plus utiliza o Network File System (NFS) para montar volumes de armazenamento para operações de backup e restauração. No Linux, assegure-se de que o cliente NFS do Linux nativo esteja instalado.

- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus podem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles deverão ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e por meio do servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.
- Se o DNS não estiver disponível, você deverá incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual do IBM Spectrum Protect Plus usando a linha de comandos.

Requisitos de autenticação e de privilégio

O IBM Spectrum Protect Plus requer privilégios de administrador usando **sudo** para várias tarefas, como descobrir layouts de armazenamento, montagem e desmontagem de discos e gerenciamento de bancos de dados. As credenciais para a VM devem especificar um usuário com os seguintes privilégios **sudo**:

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

A abordagem recomendada é criar um usuário do agente IBM Spectrum Protect Plus dedicado com os privilégios que são mostrados na configuração de amostra:

- Crie o usuário usando o comando:

```
useradd -m sppagent
```

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

- Configure uma senha usando o comando:

```
passwd sppagent_password
```

- Para ativar privilégios de superusuário para o usuário do agente, defina a configuração **!requiretty**. No final do arquivo de configuração `/etc/sudoers`, inclua as linhas a seguir:

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

Se o seu arquivo `sudoers` estiver configurado para importar configurações de outro diretório, por exemplo `/etc/sudoers.d`, você poderá adicionar as linhas no arquivo apropriado nesse diretório.

Requisitos do Sistema de arquivos



Antes de registrar o Microsoft Windows sistemas de arquivos com IBM Spectrum Protect Plus, assegure-se de que seu ambiente de sistema atenda aos requisitos destacados.

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 [Nota técnica 304861](#).

Os requisitos de backup e restauração do IBM sistemas de arquivos para o IBM Spectrum Protect Plus são os seguintes.




Configuração

Versões do Aplicativo

IBM Spectrum Protect Plus	Microsoft Windows Resilient File System (ReFS)	Microsoft New Technology File System (NTFS)
V10.1.6		

Restrição: mesmo que outros sistemas de arquivos Microsoft Windows, como a tabela de alocação (FAT), sejam detectados durante o processo de inventário, esses sistemas de arquivos não podem ser incluídos em tarefas ou protegidos.

Sistemas Operacionais

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Standard and Datacenter editions	Microsoft Windows Server 2016* Standard and Datacenter editions	Microsoft Windows Server 2019* Standard and Datacenter editions
V10.1.6			
*A liberação base e os níveis de manutenção posteriores (kernel de 64 bits) são suportados.			

O IBM Spectrum Protect Plus suporta o servidor host do proxy em execução em servidores físicos (bare metal) e em um ambiente virtualizado.

Restrictions

As seguintes restrições são aplicadas:

- O IBM Spectrum Protect Plus não protege compartilhamentos do sistema de arquivos ou volumes de cluster Microsoft.
- Os sistemas de arquivos FAT da Microsoft não são suportados.
- Os arquivos stub do Windows do IBM Spectrum Protect HSM não são suportados.
- Assegure-se de que sua configuração do sistema de arquivos não inclua pontos de montagem aninhados.
- Os compartilhamentos de rede não são locais alternativos válidos para tarefas de restauração.
- As tarefas de inventário não devem ser planejadas para serem executadas ao mesmo tempo que as tarefas de backup.

Autenticação e Privilégios

Autenticação

Para registrar um sistema de arquivos Windows, um usuário de administração do IBM Spectrum Protect Plus deve se registrar no host do cliente no qual os sistemas de arquivos a serem protegidos estão localizados.

Os servidores de arquivos Windows podem ser registrados com um ID do usuário Administrador. É possível registrar o servidor de arquivos usando um ID do usuário do domínio, se esse usuário for o administrador de domínio ou um usuário local com privilégios de administrador.

Privilégios

O ID do usuário para registrar servidores de arquivos do Windows pode ser configurado com uma das configurações do Windows a seguir:

- Desative a conta do usuário do administrador do sistema local com o componente de segurança do Controle de Conta de Usuário (UAC).
 - Abra o **Painel de Controle do Sistema do Windows > Configurações de Controle de Conta de Usuário**
 - Mova a régua de controle para **Nunca notificar**.
- Desative a configuração de política de segurança Modo de Aprovação Admin para um usuário que seja membro do Grupo de administrador local.
 - Com esse usuário, abra a **Política de Segurança Local do Sistema Windows**

- No menu **Configurações de Segurança**, escolha **Políticas Locais > Opções de Segurança > Controle de Conta de Usuário: Executar todos os Administradores** na política **Modo de Aprovação Admin**
- Desative o **Controle de Conta de Usuário: Executar todos os Administradores**
- Assegure-se de que o seu **Grupo de Administrador Local** inclua a política **Efetuar Logon como Serviço**.

Consulte também [Política de Grupo de Controle de Conta de Usuário e configurações de chave de registro](#)

Pré-requisitos e operações

Pré-requisitos

Os pré-requisitos a seguir devem ser atendidos antes de você iniciar a proteção de seus recursos. Para obter detalhes, consulte [Pré-requisitos para sistemas de arquivos](#).

- Antes de iniciar o backup de dados que são armazenados no sistema de arquivos registrado, assegure-se de que você tenha espaço livre em disco suficiente no host de backup e no repositório vSnap.
- Se você planeja restaurar dados para um local alternativo, permita um espaço extra. Nenhum arquivo é sobrescrito durante o processo de restauração. Quando os arquivos com nomes idênticos são localizados, ambas as cópias são retidas.
- Se o agente de sistemas de arquivos IBM Spectrum Protect Plus estiver em execução, um certificado autoassinado e uma chave são criados. É possível aumentar o acesso seguro para proteção de arquivos do sistema de arquivos com o IBM Spectrum Protect Plus criando um certificado e gerenciando sua colocação.

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- Para iniciar a proteção dos dados em um ReFS ou NTFS, deve-se incluir o endereço do host no qual o sistema de arquivos está localizado. É possível repetir o procedimento para incluir cada host que você deseja proteger com o IBM Spectrum Protect Plus, conforme descrito em [Incluindo um servidor de sistema de arquivos](#).
- Antes que um usuário do IBM Spectrum Protect Plus possa implementar operações de backup e de restauração, as funções e os grupos de recursos devem ser designados para o usuário. Conceda aos usuários acesso a operações de backup e de restauração usando a área de janela de Contas. Para obter instruções, consulte [Gerenciando o acesso de usuário](#).
- Configure uma política de acordo de nível de serviço (SLA). Para obter instruções, consulte [Definindo uma tarefa de backup do Acordo de Nível de Serviço](#).

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- Durante o backup inicial, o IBM Spectrum Protect Plus cria um novo volume de vSnap e compartilhamento do Common Internet File System (CIFS). Durante backups incrementais, o volume criado anteriormente é reutilizado. O agente do sistema de arquivos IBM Spectrum Protect Plus monta o compartilhamento no servidor em que o backup deve ser concluído, conforme descrito em [Fazendo backup de dados do sistema de arquivos](#).
- Em uma tarefa de backup, é possível definir regras de exclusão para excluir determinadas unidades, diretórios ou arquivos. Esses arquivos não são submetidos a backup como parte de sua política de SLA ou como parte de uma tarefa de backup ad hoc. Quando você executa uma tarefa de restauração, as regras de exclusão significam que as unidades, os diretórios ou os arquivos que são especificados nas regras de exclusão não são restaurados para a nova cópia. Para obter mais informações, consulte [Sintaxe de Regras de Exclusão](#).
- Para restaurar dados do sistema de arquivos do repositório vSnap, defina uma tarefa que restaure dados do backup mais novo ou de uma cópia de backup anterior. Você pode restaurar dados para o local original ou para um local alternativo, que pode estar em um host do cliente diferente. Você também pode especificar outras opções de recuperação, conforme descrito em [Restaurando dados do sistema de arquivos](#).

- O processo de restauração não é rastreado na página de Tarefas e Operações do IBM Spectrum Protect Plus. Use o navegador File Systems File-Level Restore para especificar as unidades, diretórios e arquivos para a tarefa. É possível definir um local alternativo para a operação de restauração e monitorar a tarefa de restauração até que ela seja concluída no navegador.
- Assegure-se de que o destino do IBM Spectrum Protect para sua tarefa de restauração esteja registrado e configurado corretamente.
- Quando a tarefa de restauração for concluída, você deverá remover o recurso da guia Recursos Ativos na janela Tarefas e Operações. Não é possível executar outra tarefa de restauração até que o recurso ativo seja cancelado.

Conectividade

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

- O adaptador de rede usado para a conexão deve ser configurado como um cliente para o Microsoft Networks.
- O serviço do Microsoft Windows Remote Management (WinRM) deve estar em execução.
- Os firewalls devem ser configurados para ativar o IBM Spectrum Protect Plus para se conectar ao servidor usando o WinRM.
- Os firewalls devem ser configurados para ativar o navegador File Systems File-Level Restore do IBM Spectrum Protect Plus para conectar-se ao serviço de restauração.
- O endereço IP do host do cliente que você registrar deve estar acessível a partir do servidor IBM Spectrum Protect Plus e do servidor vSnap. O agente de sistemas de arquivos Windows deve ter um serviço Windows Remote Management atendendo na porta 5985.
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes DNS forem usados, eles devem ser resolvíveis sobre a rede pelo servidor de dispositivo virtual IBM Spectrum Protect Plus e a partir do servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.

Portas

As portas a seguir são usadas pelos usuários dos agentes do IBM Spectrum Protect Plus.

<i>Tabela 14. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus</i>				
Porta	Protocolo	Iniciador	Resposta	Descrição
5985	Transmission Control Protocol (TCP)	Dispositivo virtual do IBM Spectrum Protect Plus ¹	Sistemas de arquivos do Windows	Fornecer acesso ao serviço do Microsoft WinRM para servidores baseados no Windows
5986	TCP	Dispositivo virtual do IBM Spectrum Protect Plus ¹	Sistemas de arquivos do Windows	Fornecer acesso ao serviço do Microsoft WinRM para servidores baseados no Windows

Tabela 14. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
9085	TCP	Navegador File Systems File-Level Restore	Sistemas de arquivos do Windows	O navegador File Systems File-Level Restore usado durante operações de restauração se conecta entre essa UI e o servidor de arquivos

¹ O dispositivo virtual IBM Spectrum Protect Plus contém os componentes de base a seguir: o servidor IBM Spectrum Protect Plus, o servidor vSnap e um proxy VADP, consulte [Componentes do produto](#).

Tabela 15. Portas de comunicação quando o inicializador for um usuário do agente do IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
445	TCP	Sistemas de arquivos do Windows	servidor vSnap	Fornece a porta de destino CIFS do servidor vSnap que é usada para montagem de compartilhamentos do sistema de arquivos para operações de backup e recuperação de log de transações

Hardware

Tabela 16. Requisitos Mínimos de Hardware

System	Espaço em disco	do NT
Hardware baseado em x86_64 compatível com uma das versões do sistema operacional Windows listadas na seção Software.	500 MB de espaço livre em disco que pode ser usado para a implementação do agente de backup.	5 GB de RAM por 1 milhão de arquivos no sistema de arquivos que deve ser protegido. Nota: O teste de escalabilidade mostrou que o módulo usado para varrer o sistema de arquivos para identificar candidatos a backup consome mais memória do que o esperado. Um APAR resolve essa limitação.

Requisitos do Suporte de Backup de Kubernetes

Antes de implementar o Suporte de Backup de Kubernetes do IBM Spectrum Protect Plus no ambiente do Kubernetes, assegure-se de que o ambiente do seu sistema atenda aos requisitos destacados.

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 [Nota técnica 304861](#).






Suporte de Backup de Kubernetes está disponível apenas em inglês no IBM Spectrum Protect Plus Versão 10.1.6.

Configuração

Versões do Aplicativo

Contêineres Docker são suportados em Suporte de Backup de Kubernetes.

Sistemas operacionais

Tabela 17. Matriz de cobertura para sistemas operacionais suportados no Linux x86_64			
IBM Spectrum Protect Plus	RHEL 7.6	RHEL 7.7	RHEL 7.8
V10.1.5			--
V10.1.6			

Requisitos adicionais

O IBM Spectrum Protect Plus V10.1.6 suporta os seguintes softwares e sistemas:

- Kubernetes 1.18 e correções e atualizações mais recentes
- Kubernetes 1.17 e correções e atualizações mais recentes
- Kubernetes 1.16 e correções e atualizações mais recentes
- Driver Ceph Container Storage Interface (CSI) 1.2, 2.0 e 2.1 com armazenamento Rados Block Device (RBD)
- Helm v2.16.1 e mais recente.

Restrição: O Helm v3 não é suportado.

Se você estiver usando as versões de driver Kubernetes e Ceph CSI a seguir, use IBM Spectrum Protect Plus V10.1.5:

- Kubernetes v1.13 e correções e atualizações mais recentes
- Kubernetes v1.14 e correções e atualizações mais recentes
- Kubernetes v1.15 e correções e atualizações mais recentes
- Driver Ceph CSI 1.1 com armazenamento RBD

Para obter informações sobre liberações de Kubernetes, consulte [Versão da Liberação do Kubernetes](#).

Para instalar e configurar o suporte de backup de contêiner, você deve implementar o software Suporte de Backup de Kubernetes no ambiente de Kubernetes. Para obter instruções, consulte [Capítulo 5, “Instalando o Suporte de Backup de Kubernetes”](#), na página 149.

Restrições

- As operações de backup para volumes de bloco bruto não são suportadas.
- Para assegurar que uma solicitação de restauração funcione corretamente, não exclua manualmente quaisquer capturas instantâneas de volumes que sejam protegidos por Suporte de Backup de Kubernetes.
- Não é possível restaurar um backup de captura instantânea ou de cópia para um espaço de nomes ou cluster diferente.

- Não é possível restaurar um backup de captura instantânea ou de cópia para o volume persistente original.
- É possível restaurar um backup de captura instantânea ou de cópia apenas para um novo volume persistente. A solicitação de volume persistente (PVC) para o novo volume é criada automaticamente durante a operação de restauração.
- Um retrocesso para uma versão anterior do Suporte de Backup de Kubernetes não é suportado. Em outras palavras, não é possível usar o Suporte de Backup de Kubernetes V10.1.5 para restaurar dados que foram submetidos a backup pelo Suporte de Backup de Kubernetes V10.1.6.
- O upgrade do produto por meio do Suporte de Backup de Kubernetes V10.1.5 não é suportado.
- Devido a mudanças subjacentes no objeto BaaSReq em Suporte de Backup de Kubernetes V10.1.6, não é possível usar Suporte de Backup de Kubernetes V10.1.6 para restaurar dados que foram submetidos a backup por Suporte de Backup de Kubernetes V10.1.5.

Software

Pré-requisitos do cluster

Assegure-se de que os seguintes pré-requisitos de cluster sejam atendidos:

- O Suporte de Backup de Kubernetes protege apenas o armazenamento persistente que foi alocado por um plug-in de armazenamento que suporta o CSI.
- Você deve estar executando um cluster de Kubernetes com suporte CSI.
- O armazenamento persistente deve ser fornecido pelo driver CSI, que deve suportar os recursos de captura instantânea do CSI.
- O suporte de captura instantânea CSI deve ser ativado na linha de comandos **kubect1**.
- A ferramenta de linha de comandos do Kubernetes **kubect1** deve estar acessível no host de instalação e no caminho local.
- Apenas os volumes formatados podem ser montados para o movedor de dados para operações de cópia.
- Opcional: para ajudar a otimizar o desempenho do produto e a escalabilidade, assegure-se de que o Kubernetes Metrics Server v0.3.5 ou posterior esteja instalado e em execução em seu cluster. Para obter instruções, consulte [“Verificando se o Metrics Server está em execução”](#) na página 150.
- Somente para Kubernetes 1.16: as operações de restauração de captura instantânea e backup de cópia requerem que o recurso alfa **VolumeSnapshotDataSource** esteja ativado. Para ativar o recurso alfa **VolumeSnapshotDataSource**, você deve corrigir o planejador de Kubernetes, o controlador e o servidor da API. Para obter instruções, consulte [“Ativando o recurso VolumeSnapshotDataSource”](#) na página 149.
- Uma classe de armazenamento deve ser definida para os volumes persistentes que estão sendo protegidos.
- O registro de imagem de destino deve ser acessível a partir do cluster de Kubernetes. O registro de imagem de destino pode ser um registro de imagem local ou um registro de imagem externo. Para um registro de imagem externo, é possível configurar o segredo de extração de imagem para proteger seu ambiente. Para obter instruções, consulte [“Criando um segredo de extração de imagem para usar com um registro externo”](#) na página 151.
- O host que é usado para instalar Suporte de Backup de Kubernetes deve estar usando um arquivo `kubeconfig` com privilégios de cluster-admin, KUBECONFIG e o cliente Helm deve estar instalado.
- Para criar novos recursos em todo o cluster, você deve estar logado no cluster de destino como um usuário com privilégios cluster-admin.
- Certifique-se de que os segredos do Suporte de Backup de Kubernetes que incluem IDs de usuário, senhas e chaves sejam criptografados inativos no armazenamento de valor da chave distribuído etc. Para obter mais informações, consulte [Criptografando Dados Secretos Inativos](#).

Pré-requisitos do Helm

- A ferramenta Helm deve ser configurada no cluster de destino para que uma nova implementação possa ser executada com a linha de comandos **helm**. A implementação de um pacote com o Helm permite que as regras de controle de acesso baseado na função (RBAC) em todo o cluster e ligações de função sejam geradas.
- Para o cluster de Kubernetes, para instalar o Helm como usuário raiz com a conta do usuário administrativo do Kubernetes, execute o script a seguir, que está incluído no pacote de instalação:

```
./helm_install_k8s.sh
```

IBM Spectrum Protect Plus pré-requisito

Componentes externos não de contêiner, como IBM Spectrum Protect Plus e o servidor vSnap IBM Spectrum Protect Plus, devem ser fornecidos e configurados pelo administrador do IBM Spectrum Protect Plus.

- Uma conta administrativa para Suporte de Backup de Kubernetes deve ser configurada no IBM Spectrum Protect Plus.

Essa conta administrativa pode ser configurada como uma conta global Lightweight Directory Access Protocol (LDAP) no data center. Essa conta global é necessária para acesso a todos os componentes externos com que o Suporte de Backup de Kubernetes opera.

Você deve especificar esse nome de conta no parâmetro BAAS_ADMIN no arquivo de configuração `baas_config.cfg` antes de implementar o Suporte de Backup de Kubernetes. O `baas_config.cfg` está localizado no diretório `installer`. Para obter instruções, consulte [“Instalando e implementando imagens do Suporte de Backup de Kubernetes no ambiente de Kubernetes”](#) na página 152.

- Uma instância do IBM Spectrum Protect Plus deve ser implementada e licenciada como um dispositivo virtual VMware.

A conectividade de rede deve existir para e a partir do cluster de destino. O endereço de IP (Internet Protocol) e o número da porta do IBM Spectrum Protect Plus devem ser especificados no arquivo `baas_config.cfg` antes de implementar o Suporte de Backup de Kubernetes. Apenas uma porta (443) pode ser especificada para uso com todas as instâncias IBM Spectrum Protect Plus.
- Uma instância do vSnap IBM Spectrum Protect Plus deve ser implementada como um dispositivo virtual VMware.
 - A conectividade de rede deve existir para e a partir do cluster de Kubernetes de destino e instância vSnap do IBM Spectrum Protect Plus.
 - A instância vSnap deve ser configurada como um servidor vSnap externo para armazenamento de backups. Para obter instruções, consulte [Capítulo 3, “Instalando servidores vSnap”](#), na página 109.
 - Se os backups forem criptografados inativos, certifique-se de que seja alocada capacidade suficiente para criptografia no servidor vSnap.

Autenticação e Privilégios

- Assegure-se de especificar o nome de usuário para a conta administrativa do IBM Spectrum Protect Plus no arquivo de configuração `baas_config.cfg`. Para obter mais informações, consulte [“Instalando e implementando imagens do Suporte de Backup de Kubernetes no ambiente de Kubernetes”](#) na página 152.
- Para acessar o dispositivo que está associado ao volume persistente, o contêiner do movedor de dados deve ser um contêiner privilegiado.
- Dependendo de sua função, os desenvolvedores de aplicativos corporativos e os administradores de backup interagem com diferentes interfaces com o usuário para proteger dados persistentes em contêineres, conforme descrito em [“Funções de Usuário”](#) na página 320.

Pré-requisitos e operações

Pré-requisitos

Assegure-se de que os requisitos do [“Software”](#) na página 56, [“Conectividade”](#) na página 58, [“Autenticação e Privilégios”](#) na página 57 sejam atendidos.

O Suporte de Backup de Kubernetes deve ser instalado no ambiente de Kubernetes, conforme descrito em [Capítulo 5, “Instalando o Suporte de Backup de Kubernetes”](#), na página 149.

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- Depois que o Suporte de Backup de Kubernetes é instalado, o host do aplicativo para o contêiner Suporte de Backup de Kubernetes é registrado automaticamente na inicialização do host do cluster em Kubernetes. Quando um cluster é registrado com IBM Spectrum Protect Plus, um inventário dos recursos no cluster é capturado automaticamente, permitindo que você conclua tarefas de backup e restauração e execute relatórios.
- Para proteger os volumes persistentes que estão conectados a um cluster de Kubernetes, crie políticas de acordo de nível de serviço (SLA) e crie tarefas para operações de backup e restauração na interface com o usuário do IBM Spectrum Protect Plus. Se você não planeja usar a política de SLA padrão para contêineres, assegure-se de configurar uma política de SLA. Para obter instruções, consulte [“Criando uma política de SLA para cluster de Kubernetes”](#) na página 242.
- Assegure-se de que funções e grupos de recursos apropriados sejam designados ao usuário que executa a tarefa de backup. 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. Para obter instruções, consulte [Capítulo 18, “Gerenciando o acesso de”](#), na página 517.
- As solicitações de backup são direcionadas a PVCs para os volumes que você deseja proteger. Antes de planejar uma tarefa de backup, tome as ações a seguir:
 - Assegure-se de que o PVC exista dentro do espaço de nomes especificado.
 - Assegure-se de que o PVC esteja formatado. Os PVCs devem ser formatados antes que possam ser submetidos a backup. Para que um PVC seja formatado corretamente, ele deve ser montado e gravado para. As operações de backup de volumes de bloco brutos não são suportadas.
 - Determine qual política de SLA atribuir a PVCs. Para obter instruções sobre como visualizar as políticas de SLA disponíveis, consulte [“Políticas de SLA”](#) na página 319.
 - Se um PVC estiver associado a múltiplas políticas de SLA, assegure-se de que as políticas não estejam planejadas para serem executadas 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.

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- É possível usar a interface com o usuário do IBM Spectrum Protect Plus para criar tarefas para operações de backup e restauração e para expirar ou monitorar tarefas do Suporte de Backup de Kubernetes e criar relatórios. Para obter instruções, consulte [“Fazendo backup e restaurando clusters Kubernetes usando a interface com o usuário do IBM Spectrum Protect Plus”](#) na página 322.
- Como um desenvolvedor de aplicativos em um ambiente de Kubernetes, é possível enviar solicitações de Suporte de Backup do Kubernetes usando a interface da linha de comandos do Kubernetes para fazer backup e restaurar dados do contêiner e para consultar o status de solicitações do Suporte de Backup de Kubernetes. Para obter instruções, consulte [“Protegendo contêineres usando a linha de comandos”](#) na página 336.

Conectividade

Assegure-se de que os requisitos de conectividade a seguir sejam atendidos:

- O subsistema de protocolo de transferência de arquivos seguro (SFTP) para o Secure Shell (SSH) está ativado.
- O serviço SSH está em execução nos serviços do Kubernetes NodePort.
- Os firewalls são configurados para permitir que IBM Spectrum Protect Plus conecte contêineres do movedor de dados usando SSH através do intervalo de portas NodePort do cluster de Kubernetes. O

serviço NodePort permite que a porta específica no intervalo de NodePort seja determinada pelo Kubernetes no tempo de execução.

- O IBM Spectrum Protect Plus usa o protocolo do Network File System (NFS) para montar volumes de armazenamento para operações de backup e de restauração. Assegure-se de que o cliente NFS do Linux nativo esteja instalado no servidor host do proxy.
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles deverão ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e pelo servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.
- Se o DNS não estiver disponível, você deverá incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual do IBM Spectrum Protect Plus usando a linha de comandos.

Portas

As portas de comunicações a seguir são usadas por agentes IBM Spectrum Protect Plus.

Tabela 18. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus				
Porta	Protocolo	Iniciador	Resposta	Descrição
Designado pelo serviço NodePort em Kubernetes	Transmission Control Protocol (TCP)	Dispositivo virtual IBM Spectrum Protect Plus ¹	Kubernetes	Usado por IBM Spectrum Protect Plus para conectar-se ao contêiner do movedor de dados para implementar e executar agentes
¹ Refere-se ao servidor IBM Spectrum Protect Plus, que é um componente do dispositivo virtual IBM Spectrum Protect Plus, conforme descrito em “Componentes do Produto” na página 6 .				

Para conexões SSH entre contêineres no ambiente de Kubernetes, a porta 22 é usada. Para todas as outras conexões, seja nos hosts de Kubernetes ou fora do cluster, utiliza-se a porta que o serviço NodePort designou no tempo de execução.

Tabela 19. Portas de comunicação quando o inicializador é o agente IBM Spectrum Protect Plus				
Porta	Protocolo	Iniciador	Resposta	Descrição
111	TCP	Kubernetes	servidor vSnap	Permite que clientes do Open Network Computing (ONC) descubram portas para comunicações com servidores ONC

Tabela 19. Portas de comunicação quando o inicializador é o agente IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
443	TCP	Kubernetes	servidor vSnap	Usado para comandos emitidos do IBM Spectrum Protect Plus para executar operações de backup, restauração, inventário e outras operações de configuração
2049	TCP	Kubernetes	servidor vSnap	Usado para transferência de dados do NFS para e de servidores vSnap
20048	TCP	Kubernetes	servidor vSnap	Monta sistemas de arquivos do vSnap em clientes como o proxy do VMware vStorage API for Data Protection (VADP), servidores de aplicativos e armazenamentos de dados de virtualização

Conceitos relacionados

[“Protegendo os contêineres”](#) na página 317

Suporte de Backup de Kubernetes é um recurso do IBM Spectrum Protect Plus que estende a proteção de dados a contêineres em clusters Kubernetes. Kubernetes é um sistema para orquestrar contêineres através de clusters de hosts.

Requisitos do Db2

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

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 [Nota técnica 304861](#).

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:

Versões do Aplicativo

Tabela 20. Matriz de cobertura para níveis do aplicativo suportados pelo IBM Spectrum Protect Plus

IBM Spectrum Protect Plus	Db2 V10.5* Enterprise Edition	Db2 V11.1* Enterprise Edition	Db2 V11.5* Enterprise Edition
V10.1.2			--
V10.1.3			--
V10.1.4			--
V10.1.5			
V10.1.6			
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.			

Sistemas operacionais

Tabela 21. Matriz de cobertura para sistemas operacionais suportados no IBM PowerPC











IBM Spectrum Protect Plus	IBM AIX 7.1*	IBM AIX 7.2*
V10.1.2		
V10.1.3		
V10.1.4		
V10.1.5		
V10.1.6		
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.		

Tabela 22. Matriz de cobertura para níveis do aplicativo suportados pelo IBM Spectrum Protect Plus



















IBM Spectrum Protect Plus	RHEL 6.8*	RHEL 7.0*	SLES 11.0 SP4*	SLES 12.0 SP1*
V10.1.2				
V10.1.3				
V10.1.4				

Tabela 22. Matriz de cobertura para níveis do aplicativo suportados pelo IBM Spectrum Protect Plus (continuação)

V10.1.5				
V10.1.6				

*A liberação base e os níveis de manutenção e modificação posteriores são suportados.

Tabela 23. Matriz de cobertura para sistemas operacionais suportados em Linux on Power Systems (little endian)

IBM Spectrum Protect Plus	RHEL 7.1*	SLES 12.0 SP1*
V10.1.4		
V10.1.5		
V10.1.6		

*A liberação base e os níveis de manutenção e modificação posteriores são suportados.

Restrições

- O IBM Db2pureScale não é suportado
- Assegure-se de que sua configuração de volume lógico Db2 não inclua pontos de montagem aninhados.
- Se você planeja proteger várias partições, o Db2 deve estar no modo de backup paralelo. O modo de backup paralelo pode ser ativado editando as variáveis de registro do Db2. Para obter mais informações, consulte Pré-requisitos para Db2. A variável de registro **DB2_PARALLEL_ACS** está disponível apenas em determinados níveis de fix pack do Db2. Se a variável **DB2_PARALLEL_ACS** não estiver disponível em sua versão, será possível atender ao requisito, especificando **DB2_WORKLOAD = SAP**.

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. Execute `sudo -V` para verificar a versão.
- **Dica:** Os pacotes bash e sudo necessários são incluídos nos sistemas operacionais Linux86_64 e Linux Power Systems (little endian) suportados.
- Instale as correções e atualizações mais recentes do Db2 em seu ambiente.
- Assegure-se de que a versão suportada do Linux x86_64, Linux Power Systems (little endian) ou AIX esteja instalada. Assegure-se de que as correções e as atualizações mais recentes estejam instaladas.
- O International Components for Unicode (libicu) RPM-package correspondente ao sistema operacional deve ser instalado.
- Assegure-se de que o valor de tamanho do arquivo efetivo `ulimit -f` para o usuário do agente IBM Spectrum Protect Plus e o usuário da instância Db2 esteja configurado como ilimitado. Como alternativa, configure o valor suficientemente alto para permitir a cópia dos arquivos maiores de banco de dados em suas tarefas de backup e restauração. Se você alterar a configuração `ulimit`, reinicie a instância do Db2 para finalizar a configuração.

- Em um ambiente Linux, dependendo da sua versão ou distribuição, certifique-se de que o pacote do utilitário `util-linux-ng` ou `util-linux` do Linux seja atual.
- **Usuários RHEL e CentOS 6:** para assegurar que o pacote `util-linux-ng` ou `util-linux` seja atual, execute o comando a seguir: `yum update package_name`.

Autenticação e Privilégios

Autenticação

- O servidor Db2 deve ser registrado com o IBM Spectrum Protect Plus usando um usuário do sistema operacional que existe no servidor Db2. O usuário então é chamado de usuário do agente *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.

Privilégios

Para usar um banco de dados Db2, um usuário do agente IBM Spectrum Protect Plus deve ter as permissões a seguir:

- Privilégios para executar comandos como usuário raiz e como um usuário proprietário do software Db2 usando o `sudo`. O IBM Spectrum Protect Plus requer esses privilégios 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 IBM Spectrum Protect Plus execute comandos sem uma senha.
 - A configuração `!requiretty` deve ser configurada, conforme descrito em [Configurando privilégios sudo para Db2](#)
- Privilégios para ler o inventário Db2 usando o comando **db21s** no diretório `/usr/local/bin`. O IBM Spectrum Protect Plus requer esses privilégios para descobrir e coletar informações sobre instâncias e bancos de dados Db2.

Pré-requisitos e operações

Pré-requisitos

Os pré-requisitos a seguir devem ser atendidos antes de você iniciar a proteção de seus recursos. Para obter detalhes, consulte [Pré-requisitos para Db2](#)

- O log de archive Db2 é ativado e o Db2 está no modo recuperável.
- Há espaço suficiente disponível no sistema de gerenciamento de banco de dados Db2, nos grupos de volumes para a operação de backup e nos volumes de destino para cópia de arquivos durante a operação de restauração. Para obter mais informações sobre os requisitos de espaço, consulte [Requisitos de espaço para proteção do Db2](#)
 - Antes de fazer backup de bancos de dados Db2, assegure-se de ter espaço livre em disco suficiente nos hosts de origem e destino e no repositório vSnap. É necessário ter espaço livre em disco extra nos grupos de volumes no host de origem para criação de capturas instantâneas do Logical Volume Manager (LVM) temporárias dos volumes lógicos em que o banco de dados Db2 e os arquivos de log estão armazenados. Para criar capturas instantâneas do LVM de um banco de dados Db2 protegido, assegure-se de que os grupos de volumes com dados do Db2 tenham espaço livre suficiente.
 - Para AIX, podem existir no máximo 15 capturas instantâneas para cada Enhanced Journaled File System (JFS2). As capturas instantâneas JFS2 internas e externas não podem existir ao mesmo tempo para o mesmo sistema de arquivos. Assegure-se de que não exista nenhuma captura instantânea interna nos volumes JFS2, uma vez que essas capturas instantâneas podem causar problemas quando o agente IBM Spectrum Protect Plus Db2 estiver criando capturas instantâneas externas.
 - Para cada volume lógico de captura instantânea do LVM ou JFS2 que contém dados, deixe pelo menos 10% 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 Db2 do IBM Spectrum Protect Plus reservará até 25% do tamanho do volume lógico de origem para o volume lógico de captura instantânea.

- Quando você estiver restaurando dados para um local alternativo, aloque volumes dedicados extras para 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 suporta 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.
- Os volumes lógicos contendo espaços de tabela do Db2 (dados e espaços de tabela temporários), o diretório de banco de dados local e os arquivos de log do Db2 são gerenciados pelo sistema Logical Volume Management (LVM2) no Linux ou pelo JFS2 no AIX. 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](#).

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- Você deve incluir o endereço do host no qual suas instâncias do Db2 estão localizadas no IBM Spectrum Protect Plus. Você pode repetir o procedimento para adicionar cada host que você deseja proteger. Se o seu ambiente do Db2 for multiparticionado com vários hosts, você deverá incluir cada host no IBM Spectrum Protect Plus. Para obter instruções, consulte [Incluindo um servidor de aplicativos Db2](#).
- Configure uma política de acordo de nível de serviço (SLA). Para obter instruções, consulte [Definindo uma tarefa de backup do Acordo de Nível de Serviço](#).
- Antes que um usuário do IBM Spectrum Protect Plus possa implementar operações de backup e de restauração, as funções e os grupos de recursos devem ser designados para o usuário. Conceda aos usuários acesso a operações de backup e de restauração usando a área de janela de Contas. Para obter instruções, consulte [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 de log para um único banco de dados Db2 com muitas tarefas de backup. Se um único banco de dados Db2 for adicionado a várias definições de tarefa com backup de log ativado, um backup de log de uma tarefa poderá truncar um log antes de ele ser submetido a backup pela próxima tarefa. Esse truncamento pode fazer com que as tarefas de restauração point-in-time falhem.
- 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 você planeja restaurar bancos de dados multiparticionados para um local alternativo, certifique-se de que a instância de destino esteja configurada com os mesmos números de partição da instância original. Todas as 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.

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- Defina regularmente tarefas de backup planejadas do Db2 para proteger seus dados. Você também ativa operações de backup contínuo para logs de archive para poder restaurar uma cópia point-in-time com opções de rollforward, se necessário. Para obter instruções, consulte [Fazendo backup de dados do Db2](#).

- Para restaurar os dados do Db2 do repositório vSnap, defina uma tarefa que restaure dados do backup mais novo ou uma cópia de backup anterior. Você pode optar por restaurar dados para a instância original ou para uma instância alternativa em um host de cliente diferente. Para obter instruções, consulte [Restaurando dados do Db2](#).

Conectividade

Assegure-se de que os requisitos de conectividade a seguir sejam atendidos:

- O subsistema de protocolo de transferência de arquivos seguro (SFTP) para o Secure Shell (SSH) está ativado.
- O serviço do Secure Shell (SSH) está em execução na porta 22 no servidor host do proxy.
- Os firewalls são configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor host do proxy usando o SSH.
- O IBM Spectrum Protect Plus usa o protocolo do Network File System (NFS) para montar volumes de armazenamento para operações de backup e de restauração.
 - No Linux, assegure-se de que o cliente NFS do Linux nativo esteja instalado no servidor host do proxy.
 - No AIX, assegure-se de que a comunicação NFS esteja configurada com portas reservadas usando o seguinte comando:


```
nfsd -p -o nfs_use_reserved_port=1
```
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles devem ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e pelo servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.
- Se o DNS não estiver disponível, você deverá incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual IBM Spectrum Protect Plus usando a linha de comandos.

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus.

Tabela 24. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus				
Porta	Protocolo	Iniciador	Resposta	Descrição
22	Transmission Control Protocol (TCP)	Dispositivo virtual do IBM Spectrum Protect Plus ¹	Db2 Server	Fornece acesso para solucionar problemas e manter servidores host do proxy remotos executando componentes de aplicativo guest usando o protocolo SSH
¹ O dispositivo virtual do IBM Spectrum Protect Plus contém os seguintes componentes de base: servidor IBM Spectrum Protect Plus, servidor vSnap e um proxy VADP, conforme descrito em Componentes do produto .				

Tabela 25. Portas de comunicação quando o iniciador é o agente IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
111	TCP	Db2 Server	servidor vSnap	Permite que clientes do Open Network Computing (ONC) descubram portas para comunicações com servidores ONC
2049	TCP	Db2 Server	servidor vSnap	Usado para transferência de dados do NFS para e de servidores vSnap
20048	TCP	Db2 Server	servidor vSnap	Monta sistemas de arquivos do vSnap em clientes como o proxy do VMware vStorage API for Data Protection (VADP), servidores de aplicativos e armazenamentos de dados de virtualização

Hardware

Tabela 26. Requisitos Mínimos de Hardware

System	Espaço em Disco
Hardware compatível que é suportado pelo sistema operacional e pelo servidor de banco de dados Db2	Um mínimo de 500 MB de espaço em disco para o produto a ser instalado

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 [Nota técnica 304861](#).

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

Configuração

Versões do Aplicativo

Tabela 27. Matriz de cobertura para níveis de aplicação suportados por IBM Spectrum Protect Plus

IBM Spectrum Protect Plus	Microsoft Exchange Server 2013 CU16* Standard e Enterprise Editions	Microsoft Exchange Server 2016 CU5* Standard e Enterprise Editions	Microsoft Exchange Server 2019* Standard e Enterprise Editions
V10.1.3	✓	✓	✓
V10.1.4	✓	✓	✓
V10.1.5	✓	✓	✓
V10.1.6	✓	✓	✓
* A liberação base e as atualizações acumulativas posteriores e os níveis de manutenção são suportados.			

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

Sistemas Operacionais

Tabela 28. Matriz de cobertura para sistemas operacionais suportados no Windows x64

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Edições padrão e de data center	Microsoft Windows Server 2016* Edições padrão e de data center	Microsoft Windows Server 2019* Edições padrão e de data center
V10.1.3	✓	✓	✓
V10.1.4	✓	✓	✓
V10.1.5	✓	✓	✓
V10.1.6	✓	✓	✓
* A liberação base e os níveis de manutenção posteriores são suportados.			

O IBM Spectrum Protect Plus suporta o Microsoft Exchange Server em execução em um servidor físico (bare metal) e em um ambiente virtualizado. Os ambientes virtualizados a seguir são suportados:

- Sistema operacional guest VMware Elastic Sky X (ESX)
- Microsoft Windows Hyper-V guest sistema operacional

Consulte requisitos mínimos para ativar o rastreamento de faixa de gravação em [“Backups incrementais”](#) na página 70.

Restrições

As seguintes restrições são aplicadas:

- O Windows Server 2019 com a opção Server Core é suportado. No entanto, o recurso de restauração granular não é suportado pela opção de instalação do Server Core.
- Os logs do banco de dados são submetidos a backup somente no nó preferencial. Apenas uma instância do Exchange Server por vez pode gravar backups de log no servidor vSnap.
- Ao restaurar um item de caixa postal (ou caixa postal) para um arquivo de pastas pessoais (.pst) do Outlook, é possível usar a visualização do Mailbox Restore Browser somente com arquivos .pst não Unicode.
- Ao restaurar um item de caixa postal (ou caixa postal) para uma caixa postal diferente, não será possível arrastar itens de correio ou subpastas na pasta Itens Recuperáveis para uma caixa de correio de destino.
- Ao restaurar itens de correio para um arquivo de pastas pessoais não Unicode (.pst), cada pasta pode conter um máximo de 16.383 itens de correio.

Consulte restrições específicas para tecnologias que não são suportadas para rastreamento de bytes alterados em [“Backups incrementais” na página 70](#).

Software

- Instale as correções e atualizações do banco de dados Microsoft Exchange mais recente em seu ambiente.
- Instale uma versão suportada de um sistema operacional Windows de 64 bits em seu ambiente. Assegure-se de que as correções e as atualizações mais recentes estejam instaladas.
- O software a seguir deve ser instalado antes de usar o IBM Spectrum Protect Plus:
 - Windows PowerShell 4 ou posterior
 - Windows Management Framework 4 ou posterior
- Se você usar o Microsoft Exchange Server 2013 com o recurso de restauração granular, o nível mínimo suportado para o Microsoft Exchange Messaging API (MAPI) Client and Collaboration Data Objects (CDO) é versão 6.5.8320.0.
- Se você usar o recurso de restauração granular com o Microsoft Exchange Server 2016 ou 2019, o Microsoft 32-bit Outlook 2013, Outlook 2016 ou Outlook 2019 será necessário.
- O software a seguir, requerido pela Microsoft, é instalado automaticamente pelo recurso de restauração granular IBM Spectrum Protect Plus, se ainda não estiver presente em sua máquina virtual:
 - 32-bit Microsoft Visual C++ 2012 Redistributable Package
 - 64-bit Microsoft Visual C++ 2012 Redistributable Package
 - 32-bit Microsoft Visual C++ 2017 Redistributable Package
 - 64-bit Microsoft Visual C++ 2017 Redistributable Package
 - Microsoft .NET Framework 4.5
 - Microsoft ReportViewer 2012 SP1 Redistributable Package
 - Microsoft SQL Server 2012 System CLR Types
 - Microsoft SQL Server 2014 System CLR Types
 - Microsoft SQL Server 2016 System CLR Types

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

Autenticação e Privilégios

Autenticação

Registre cada Microsoft Exchange Server com IBM Spectrum Protect Plus por nome ou endereço IP.

Restrição: O endereço IP deve ser acessível por meio do servidor IBM Spectrum Protect Plus e por meio do servidor vSnap. O nome completo do domínio de cada Microsoft Exchange Server deve ser resolvível e pode ser roteado a partir do servidor IBM Spectrum Protect Plus e do servidor vSnap. O nome completo do domínio do servidor IBM Spectrum Protect Plus deve ser resolvível e pode ser roteado a partir dos servidores Microsoft Exchange.

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

Privilégios

Para usar um banco de dados do Exchange, um usuário do agente IBM Spectrum Protect Plus deve ter os privilégios apropriados. Para obter instruções sobre como atribuir privilégios, consulte [“Privilégios” na página 391](#).

Revise as informações a seguir sobre privilégios e restrições:

- Para gerenciar os grupos de funções do Exchange usando o Exchange Admin Center (EAC) ou o Exchange Powershell Cmdlets, o nome de usuário deve ser autorizado pela política de segurança.
- O Sistema de Arquivos de Criptografia (EFS) deve ser ativado na política de domínio local ou de grupo e um certificado do Agente de Recuperação de Dados de Domínio (DRA) válido deve estar disponível.
- Para usar o navegador de caixa postal para operações de restauração granular, os certificados digitais do Exchange devem estar instalados e configurados.

Dica: Com o Microsoft Exchange Server 2016 e 2019, o Exchange Server é configurado para usar Segurança da Camada de Transporte (TLS) por padrão. Esta segurança do TLS criptografa a comunicação entre servidores Exchange internos e entre os serviços do Exchange no servidor local.

Pré-requisitos e operações

Pré-requisitos

Assegure-se de que os requisitos do [“Software” na página 68](#), [“Conectividade” na página 70](#) e [“Autenticação e Privilégios” na página 68](#) sejam atendidos.

Os pré-requisitos a seguir devem ser atendidos antes de você iniciar a proteção de seus recursos. Para obter detalhes, consulte a seção [“Pré-requisitos para o Exchange Server” na página 391](#).

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- Assegure-se de que os servidores de aplicativos que contiverem os bancos de dados do Exchange dos quais você deseja fazer backup estejam registrados com o IBM Spectrum Protect Plus. Para obter instruções, consulte [“Incluindo um servidor de aplicativos do Exchange” na página 393](#).
- Configure uma política de acordo de nível de serviço (SLA). Para obter instruções, consulte [“Definindo uma tarefa de backup de Acordo de Nível de Serviço” na página 395](#).
- Assegure-se de que funções apropriadas e grupos de recursos sejam designados ao usuário que criará tarefas de backup e restauração. Para obter instruções, consulte [Capítulo 18, “Gerenciando o acesso de”, na página 517](#).

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- 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. Para obter instruções, consulte [“Fazendo backup de bancos de dados do Exchange” na página 394](#).
- Ao restaurar arquivos de um archive IBM Spectrum Protect, os arquivos são migrados inicialmente do armazenamento em fita para um conjunto de armazenamento temporário. Dependendo do tamanho dos arquivos a serem restaurados, esse processo pode levar várias horas.

- Se você planeja restaurar a restauração de dados para uma instância alternativa ou para um novo local de arquivo, os diretórios de destino que você inserir no campo **Caminho de Destino** devem existir no host de aplicativos. Se os diretórios não existirem no servidor, você deverá criá-los antes de concluir a operação de restauração.
- Se os dados em um banco de dados do Exchange forem perdidos ou corrompidos, será possível restaurar os dados por meio de uma cópia de backup. Use o assistente de "Restauração" para configurar um planejamento de tarefa de restauração ou uma operação de restauração on demand. É possível definir uma tarefa que restaure dados para a instância original. Para obter instruções, consulte [Restaurando bancos de dados do Exchange](#)

Para obter requisitos e restrições detalhadas que se aplicam a tarefas de backup, consulte [Backups incrementais](#)

Backups incrementais

O IBM Spectrum Protect Plus usa a tecnologia de diário de mudanças update sequence number (USN) para backups incrementais em um ambiente Microsoft Exchange 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.

Para ativar o rastreamento do intervalo de gravação, o ambiente do sistema deve atender aos requisitos a seguir:

- Windows Server 2012 R2 ou mais recente
- New Technology File System (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
- Transparent Failover (TFO) do SMB
- SMB 3.0 with Scale-out file shares

Por padrão, 512 MB de espaço são alocados para registro no diário de mudança de USN. Além disso, quando o estouro do diário é detectado, o espaço alocado dobra de tamanho, para um máximo de 2 GB.

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.

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

- A descontinuidade do diário é relatada. Esse problema pode ocorrer quando o log atinge seu tamanho máximo, quando o registro de diário é desativado ou quando o ID USN catalogado é alterado.
- O tamanho do arquivo é menor que ou igual ao tamanho do limite de rastreamento, que por padrão é 1 MB.
- Um arquivo é incluído após uma operação de backup anterior.

Conectividade

Assegure-se de que os requisitos de conectividade a seguir sejam atendidos:

- O adaptador de rede usado para a conexão deve ser configurado como um cliente para o Microsoft Networks.
- O serviço do Microsoft Windows Remote Management (WinRM) deve estar em execução.
- Os firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor usando o WinRM.
- O endereço IP do host do cliente que você registra deve ser alcançável a partir do servidor IBM Spectrum Protect Plus e do servidor vSnap. O servidor Microsoft Exchange deve ter um serviço WinRM atendendo na porta 5985.

- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles deverão ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e por meio do servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus.

<i>Tabela 29. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus</i>				
Porta	Protocolo	Iniciador	Resposta	Descrição
5985	Transmission Control Protocol (TCP)	Dispositivo IBM Spectrum Protect Plus ¹	Microsoft Exchange Server	Fornecer acesso ao serviço do Microsoft WinRM para servidores baseados no Windows
5986	TCP	Dispositivo IBM Spectrum Protect Plus ¹	Microsoft Exchange Server	Fornecer acesso ao serviço do Microsoft WinRM para servidores baseados no Windows

¹ O dispositivo virtual do IBM Spectrum Protect Plus contém os componentes de base a seguir: o servidor IBM Spectrum Protect Plus, o servidor vSnap e um proxy do VADP, conforme descrito em [“Componentes do Produto”](#) na página 6.

<i>Tabela 30. Portas de comunicação quando o inicializador for um usuário do agente do IBM Spectrum Protect Plus</i>				
Porta	Protocolo	Iniciador	Resposta	Descrição
3260 O inicializador iSCSI é necessário nesse nó.	TCP	Microsoft Exchange Server	servidor vSnap	A porta de destino do vSnap do serviço Microsoft Internet Small Computer System Interface (iSCSI) Initiator que é usada para montagem de LUNS para operações de backup e recuperação
443	TCP	Microsoft Exchange Server	Dispositivo IBM Spectrum Protect Plus ¹	Porta que permite que o agente se comunique com IBM Spectrum Protect Plus para enviar alertas em caso de falhas de backup do log

Tabela 30. Portas de comunicação quando o inicializador for um usuário do agente do IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
445	TCP	Microsoft Exchange Server	servidor vSnap	Fornecer a porta de destino do SMB ou do CIFS do servidor vSnap que é usada para montar compartilhamentos do sistema de arquivos para operações de backup e recuperação do log de transações

¹ O dispositivo virtual do IBM Spectrum Protect Plus contém os componentes de base a seguir: o servidor IBM Spectrum Protect Plus, o servidor vSnap e um proxy do VADP, conforme descrito em [“Componentes do Produto”](#) na página 6.

Atualização de portas:

- Para Microsoft Exchange Server, a porta 443 está disponível em IBM Spectrum Protect Plus V10.1.4 e posterior.
- Em versões anteriores, as portas 137, 138 e 139 no servidor vSnap foram usadas por agentes de aplicativo que usam o SMBv1. Iniciando com o IBM Spectrum Protect Plus V10.1.6, o protocolo do SMBv1 não é usado. Todos os agentes usam o SMBv2 ou mais recente, que não requer as portas 137, 138 ou 139.

Hardware

Tabela 31. Requisitos Mínimos de Hardware

System	Espaço em disco	Espaço em disco para operações de restauração granular
Hardware compatível que é suportado pelo sistema operacional de 64 bits e o Microsoft Exchange Server	Um mínimo de 500 MB de espaço em disco para o produto a ser instalado	Pelo menos 2.1 GB de espaço em disco para o software Microsoft necessário, que é instalado automaticamente

Requisitos do MongoDB

A partir do IBM Spectrum Protect Plus V10.1.3, o suporte foi incluído para backup e restauração de dados do banco de dados MongoDB. Antes de registrar um servidor de aplicativos MongoDB com IBM Spectrum Protect Plus, assegure-se de que o ambiente do sistema atenda aos requisitos a seguir.

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 [Nota técnica 304861](#).

Requisitos de configuração

Versões do Aplicativo

Tabela 32. Matriz de cobertura para níveis de aplicativo suportados pelo IBM Spectrum Protect Plus

IBM Spectrum Protect Plus	MongoDB V3.6* Community Server and Enterprise Server editions	MongoDB V4.0* Community Server and Enterprise Server editions	MongoDB V4.2* Community Server and Enterprise Server editions
V10.1.3	✓	✓	--
V10.1.4	✓	✓	--
V10.1.5	✓	✓	--
V10.1.6	✓	✓	✓
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.			

Sistemas operacionais



Tabela 33. Matriz de cobertura para sistemas operacionais suportados no Linux x86_64

IBM Spectrum Protect Plus	RHEL 6.8*	RHEL 7.0*	CentOS 6.8*	CentOS 7.0*	SLES 12.0 SP1*
V10.1.3	✓	✓	✓	✓	✓
V10.1.4	✓	✓	✓	✓	✓
V10.1.5	✓	✓	✓	✓	✓
V10.1.6	✓ IT322842: Consulte as restrições	✓	✓ IT322842: Consulte as restrições	✓	✓
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.					

Tabela 34. Matriz de cobertura para sistemas operacionais suportados no Linux on Power Systems (little endian)

IBM Spectrum Protect Plus	RHEL 7.1*	CentOS 7.0*
V10.1.4	✓	✓
V10.1.5	✓	✓

Tabela 34. Matriz de cobertura para sistemas operacionais suportados no Linux on Power Systems (little endian) (continuação)

IBM Spectrum Protect Plus	RHEL 7.1*	CentOS 7.0*
V10.1.6	 IT322842: Consulte as restrições	 IT322842: Consulte as restrições
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.		

Proteja o ambiente MongoDB com o IBM Spectrum Protect Plus quando estiver em execução em um dos seguintes sistemas operacionais guest:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server Kernel-based Virtual Machine (KVM)

Restrições

- Todas as instâncias do MongoDB sem autenticação do usuário ativadas ainda são suportadas para todos os sistemas operacionais listados. A partir do APAR IT32842, devido a problemas com credenciais criptografadas, as instâncias do MongoDB com autenticação de usuário ativada não podem ser suportadas no IBM Spectrum Protect Plus V10.1.6 nos sistemas operacionais a seguir:
 - Linux x86_64: RHEL 6.8 e níveis de manutenção e modificação posteriores, CentOS 6.8 e níveis de manutenção e modificação posteriores
 - Linux on Power Systems: RHEL7.1 e níveis de manutenção e modificação posteriores, CentOS 7.0 e níveis de manutenção e modificação posteriores
- No Linux on Power Systems (little endian), apenas o MongoDB Enterprise Server Edition é suportado.
- As configurações de cluster compartilhadas do MongoDB são detectadas quando você executa um inventário, mas esses recursos não são elegíveis para operações de backup ou restauração.
- No MongoDB, a criptografia baseada em SSL e a autenticação baseada em certificado não são suportadas.
- Não execute tarefas de inventário durante as tarefas de backup planejadas.
- Não configure os pontos de montagem aninhados.

Software

- Os pacotes bash e sudo devem ser instalados. O Sudo deve estar na versão 1.7.6p2 ou mais recente. Execute `sudo -V` para verificar a versão.

Dica: Os pacotes bash e sudo necessários estão incluídos nos sistemas operacionais Linux x86_64 e Linux on Power Systems (little endian).
- Instale as correções e atualizações mais recentes do MongoDB em seu ambiente.
- Assegure-se de que uma versão suportada do Linux x86_64 ou do Linux on Power Systems (little endian) esteja instalada. Assegure-se de que as correções e as atualizações mais recentes estejam instaladas.
- O International Components for Unicode (**libicu**) RPM-package correspondente ao sistema operacional deve ser instalado.
- Assegure-se de que `ulimit -f`, para o usuário do agente do IBM Spectrum Protect Plus e usuário da instância do MongoDB, esteja configurado para unlimited. Como alternativa, configure um valor suficientemente alto para suportar a cópia dos arquivos maiores de banco de dados em suas tarefas de backup e restauração. Se você alterar a configuração `ulimit`, reinicie a instância do MongoDB para finalizar a configuração.
- Em um ambiente Linux, dependendo da sua versão ou distribuição, certifique-se de que o pacote do utilitário `util-linux-ng` ou `util-linux` do Linux seja atual.

- **Usuários do RHEL e CentOS 6:** para assegurar que o pacote `util-linux-ng` ou `util-linux` seja atual, execute o comando a seguir substituindo o nome do pacote no lugar de `package_name`:

```
yum update package_name
```

- **Usuários do RHEL e CentOS 6:** quando o servidor de aplicativos MongoDB executar RHEL 6 ou CentOS 6, assegure-se de que o pacote `openssl` esteja na versão 1.0.1e-57 ou posterior. Para atualizar a versão, execute o comando a seguir:

```
yum update openssl
```

Autenticação e Privilégios

Autenticação

- O servidor MongoDB deve ser registrado com o IBM Spectrum Protect Plus usando um usuário do sistema operacional que existe no servidor MongoDB. O usuário é então referido como o 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.
- Com o MongoDB Enterprise Server Edition, apenas o mecanismo de armazenamento criptografado é suportado.

Privilégios

Para usar um banco de dados MongoDB, um usuário do agente do IBM Spectrum Protect Plus deve ter as permissões a seguir:

- Privilégios para executar comandos como usuário raiz e como um usuário proprietário do software MongoDB usando o `sudo`. O IBM Spectrum Protect Plus requer esses privilégios 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 IBM Spectrum Protect Plus execute comandos sem uma senha.
 - A configuração `!requiretty` deve ser especificada, consulte a descrição em [“Configurando Privilégios Sudo”](#) na página 436.
- Privilégios para ler o módulo do servidor MongoDB padrão `/usr/local/bin/mongod`. O IBM Spectrum Protect Plus requer esses privilégios para usar a API do PyMongo para conectar-se aos servidores MongoDB usando o nome de DNS (Sistema de Nomes de Domínio) ou porta e nome do endereço IP (protocolo da Internet) designados da instância. Esse mecanismo é usado para reunir informações sobre instâncias e bancos de dados do MongoDB.
- Se o servidor MongoDB estiver protegido por autenticação baseada em função, você deverá configurar os privilégios apropriados, conforme descrito em [“Roles para MongoDB”](#) na página 434.

Pré-requisitos e operações

Pré-requisitos

Assegure-se de que o [“Software”](#) na página 74, [“Conectividade”](#) na página 76 e [“Autenticação e Privilégios”](#) na página 75 e requisitos sejam atendidos.

Os pré-requisitos a seguir devem ser atendidos antes de você iniciar a proteção de seus recursos. Para obter detalhes, consulte a seção [“Pré-requisitos para o MongoDB”](#) na página 433.

- O MongoDB é configurado como uma instância independente ou conjunto de réplicas. Os backups de instâncias de cluster fragmentadas de MongoDB não são suportados. Um backup sempre inclui todos os bancos de dados na instância.
- A instância do MongoDB está configurada para usar o WiredTiger Storage Engine.
- Cada instância do MongoDB a ser protegida deve ser registrada com IBM Spectrum Protect Plus. Depois que as instâncias são registradas, IBM Spectrum Protect Plus executa um inventário para detectar

recursos do MongoDB. Certifique-se de que todas as instâncias que você deseja proteger sejam detectadas e listadas corretamente.

- O usuário no registro do servidor de aplicativos MongoDB em IBM Spectrum Protect Plus deve ser capaz de recuperar informações do servidor e status do banco de dados admin MongoDB.
- Assegure-se de que você tenha espaço livre suficiente nos hosts de destino e de origem e no repositório vSnap. É necessário espaço extra para armazenar backups temporários do Logical Volume Manager (LVM) de volumes lógicos em que os dados do MongoDB estão localizados. Esses backups temporários, conhecidos como capturas instantâneas LVM, são criados automaticamente pelo agente do MongoDB. Para cada volume lógico de captura instantânea do LVM, pelo menos 10% de espaço livre devem ser alocados no grupo de volumes. Se houver espaço livre suficiente no grupo de volumes, o agente do MongoDB IBM Spectrum Protect Plus reserva até 25% do tamanho do volume lógico de origem para o volume lógico de captura instantânea. Para obter mais informações, consulte [“Pré-requisitos de espaço para a proteção de MongoDB”](#) na página 435.
- Certifique-se de que espaço em disco suficiente seja alocado no servidor de destino para operações de restauração.
- Os volumes lógicos de dados do MongoDB e os caminhos de log são gerenciados pelo Linux Logical Volume Manager (LVM2). O LVM2 é usado para criar capturas instantâneas de volume temporário. Os arquivos do banco de dados e o diário devem estar em um único volume. O volume lógico aumenta de tamanho com os dados, já que os dados mudam no volume de origem enquanto a captura instantânea existe. Para obter mais informações, consulte [“Linux LVM2 ”](#) na página 435.

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- Inclua os servidores de aplicativos dos quais você deseja fazer backup. Para obter instruções, consulte [“Incluindo um servidor de aplicativos MongoDB”](#) na página 436.
- Configure uma política de acordo de nível de serviço (SLA). Para obter instruções, consulte [“Definindo uma tarefa de acordo de nível de serviço regular”](#) na página 442.
- Antes que um usuário do IBM Spectrum Protect Plus possa configurar operações de backup e restauração, as funções e os grupos de recursos devem ser designados ao usuário. Conceda aos usuários acesso a recursos e operações de backup e restauração, utilizando a área de janela Contas. Para obter mais informações, consulte [Capítulo 18, “Gerenciando o acesso de”](#), na página 517 e [“Roles para MongoDB”](#) na página 434.

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- Para fazer backup regularmente de seus dados, defina uma tarefa de backup que inclua uma política de SLA. Para obter instruções, consulte [“Fazendo backup de dados do MongoDB”](#) na página 440.
- Para restaurar dados, defina uma tarefa que restaure dados do backup mais recente ou selecione uma cópia de backup anterior. É possível restaurar dados para a instância original ou para uma instância alternativa em um host de cliente 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. Para obter instruções, consulte [“Restaurando Dados do MongoDB ”](#) na página 445.
- Assegure-se de que volumes dedicados sejam alocados para cópia de arquivo.
- Assegure-se de que a mesma estrutura de diretórios e layout estejam disponíveis nos servidores de destino e de origem.
- Se você restaurar dados de um archive do IBM Spectrum Protect, os arquivos serão migrados inicialmente do armazenamento de fita para o conjunto de armazenamento temporário. Dependendo do tamanho dos arquivos a serem restaurados, esse processo pode levar várias horas.
- Para operações de restauração para instâncias alternativas, o MongoDB deve estar no mesmo nível de versão nos hosts de destino e cliente.

Conectividade

Assegure-se de que os requisitos de conectividade a seguir sejam atendidos:

- O subsistema de protocolo de transferência de arquivos seguro (SFTP) para o Secure Shell (SSH) está ativado.
- O serviço do Secure Shell (SSH) está em execução na porta 22 no servidor host do proxy.
- Os firewalls são configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor host do proxy usando o SSH.
- O IBM Spectrum Protect Plus usa o protocolo do Network File System (NFS) para montar volumes de armazenamento para operações de backup e de restauração. Assegure-se de que o cliente NFS do Linux nativo esteja instalado no servidor host do proxy.
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles deverão ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e pelo servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.
- Se o DNS não estiver disponível, você deverá incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual do IBM Spectrum Protect Plus usando a linha de comandos.

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus.

Tabela 35. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
22	Transmission Control Protocol (TCP)	Dispositivo virtual IBM Spectrum Protect Plus ¹	MongoDB	Fornece acesso para solucionar problemas e manter servidores host do proxy remotos executando componentes do aplicativo guest usando o protocolo SSH.

¹ O dispositivo virtual IBM Spectrum Protect Plus contém os componentes de base: servidor IBM Spectrum Protect Plus, site, servidor vSnap e proxy VADP, conforme descrito em [“Componentes do Produto”](#) na página 6.

Tabela 36. Portas de comunicação quando o inicializador é o agente IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
111	TCP	MongoDB	servidor vSnap	Permite que clientes Open Network Computing (ONC) descubram portas para comunicações com servidores ONC.

Tabela 36. Portas de comunicação quando o inicializador é o agente IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
2049	TCP	MongoDB	servidor vSnap	Usado para transferência de dados NFS para e a partir de servidores vSnap.
20048	TCP	MongoDB	servidor vSnap	Monta sistemas de arquivos de vSnap em clientes, como o proxy VMware vStorage API for Data Protection (VADP), servidores de aplicativos e armazenamentos de dados de virtualização.

Hardware

Tabela 37. Requisitos Mínimos de Hardware

System	Espaço em Disco
Hardware compatível que é suportado pelo sistema operacional e MongoDB.	No mínimo 500 MB de espaço em disco para o produto a ser instalado.

Requisitos do Office 365

Este documento detalha os requisitos de backup e restauração do Microsoft Office 365 para IBM Spectrum Protect Plus. Antes de registrar um host de proxy com IBM Spectrum Protect Plus, assegure-se de que o ambiente do sistema atenda aos requisitos a seguir. O servidor host do proxy é referido na interface com o usuário (UI) como o *servidor de aplicativos*.

Configuração do serviço em nuvem

A partir do IBM Spectrum Protect Plus V10.1.5, o suporte foi incluído para backup e restauração de dados do Microsoft Office 365.

Se você optar por proteger o Microsoft Office 365 com o IBM Spectrum Protect Plus, você precisa comprar IBM Spectrum Protect Plus para o Microsoft Office 365. Para obter mais informações sobre essa titularidade, consulte a carta de anúncio do [IBM Spectrum Protect V10.1.5](#).

Atualização do nome do produto: Microsoft Corporation anunciou novos nomes de produtos, em vigor a partir de 21 de abril de 2020, para suas ofertas Office 365 para pequenas e médias empresas. Com esse anúncio, todos os planos de negócios de pequeno e médio portes fizeram a transição para a nova marca Microsoft 365. No IBM Spectrum Protect Plus V10.1.6, a interface com o usuário e a documentação usam o nome do produto original, Office 365. Para obter mais informações, consulte [Novidades nas ofertas do Microsoft 365 para pequenas e médias empresas](#)

Antes de registrar um servidor host do proxy com o IBM Spectrum Protect Plus, assegure-se de que o ambiente do sistema atenda aos requisitos a seguir.

Configuração

Serviço em nuvem

Para proteger um aplicativo do Microsoft Office 365, deve-se registrar o aplicativo com o Azure Active Directory e conceder permissões apropriadas. Para começar, você deve ter os seguintes itens:










- Uma assinatura ativa do Microsoft Office 365
- Um ID do usuário administrativo e uma senha do Microsoft Office 365

Para obter instruções, consulte [Registrando com o Azure Active Directory](#).






Se você tiver uma conta administrativa do Microsoft Office 365, é possível incluir usuários para assegurar que eles tenham licenças válidas. Para obter instruções, consulte [Microsoft 365 em inscrições do Visual Studio](#).

Nota: O servidor e o usuário do servidor IBM Spectrum Protect Plus não armazenam IDs de usuários administrativos e senhas para o locatário do Microsoft Office 365.

Versões do Aplicativo

Tabela 38. Matriz de cobertura para níveis do aplicativo suportados pelo IBM Spectrum Protect Plus					
IBM Spectrum Protect Plus	Microsoft 365 Business Basic, Business Standard, Business Premium editions	Edições E1, E3 e E5 do Office 365 for Enterprise	Edições A1, A3 e A5 do Office365 for Education	Edição F3 do Office 365 for Firstline Workers	Edições E3 e E5 do Microsoft 365 for Enterprise
	Antigo nome do produto: Office 365 Business: edições Business, Essentials e Business Premium		Antigo nome do produto: Office 365 Education edition	Antigo nome do produto: Microsoft 365 F1	
V10.1.5					
V10.1.6					

Sistemas operacionais

Tabela 39. Matriz de cobertura para sistemas operacionais suportados no Linux x86_64			
IBM Spectrum Protect Plus	RHEL 7.0*	RHEL 8.0*	CentOS 7.0*
V10.1.5		--	
V10.1.6			
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.			

O IBM Spectrum Protect Plus suporta o servidor host do proxy em execução no servidor físico (bare metal) e em um ambiente virtualizado.

Restrições

O locatário do Microsoft Office 365 deve estar em uma região global, conforme definido pela Microsoft. As regiões nacionais não são suportadas. Para obter mais informações sobre regiões, consulte [implementações na nuvem nacional](#).

Software

- Assegure-se de que Java™ 8 esteja instalado.
- Os pacotes bash e sudo devem ser instalados. O Sudo deve estar na versão 1.7.6p2 ou mais recente. Executar sudo -V para verificar a versão. Dica: os pacotes bash e sudo necessários são incluídos no sistema operacional Linux x86_64 suportado.
- Instale as correções e atualizações mais recentes do Microsoft Office 365 em seu ambiente.
- Instale uma versão suportada do Linux x86_64 em seu ambiente.
- Assegure-se de que as correções e as atualizações mais recentes estejam instaladas. O International Components for Unicode (libicu) RPM-package deve ser instalado para a versão correspondente do seu sistema operacional. Assegure-se de que o valor de ulimit-f do tamanho do arquivo efetivo, que especifica o tamanho do arquivo efetivo para o agente IBM Spectrum Protect Plus, seja configurado como ilimitado. Alternativamente, configure o valor suficientemente alto para suportar a cópia dos arquivos maiores do Office 365 em suas tarefas de backup e restauração.
- Em um ambiente Linux, dependendo de sua versão ou distribuição, assegure-se de que o pacote do utilitário Linux, util-linux-ng ou util-linux, seja atual.

Autenticação e Privilégios

Autenticação

- O servidor host do proxy deve ser registrado com o IBM Spectrum Protect Plus usando um usuário do sistema operacional que existe no host do agente. O usuário é então referido como o usuário do agente 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.

Privilégios

O usuário do agente IBM Spectrum Protect Plus deve ter privilégios para executar comandos como usuário raiz usando o sudo. A configuração **sudoers** deve permitir que o usuário do agente IBM Spectrum Protect Plus execute comandos sem uma senha.

Pré-requisitos e operações

Pré-requisitos

Os pré-requisitos a seguir devem ser atendidos antes de você iniciar a proteção de seus recursos:

- Para proteger um aplicativo Office 365, deve-se registrar o aplicativo com o Azure Active Directory e conceder permissões apropriadas. Quando você registrar um novo aplicativo com o Azure Active Directory, as credenciais do aplicativo como ID do aplicativo e o segredo do aplicativo serão disponibilizadas no portal do Azure Active Directory. Para obter instruções, consulte Registrando com o Azure Active Directory
- Para assegurar que o agente IBM Spectrum Protect Plus possa se conectar ao locatário do Office 365, deve-se registrar as credenciais do locatário do Office 365 e o servidor host do proxy com o IBM Spectrum Protect Plus. Esse procedimento é necessário para assegurar que os dados do Office 365 possam ser submetidos a backup para o IBM Spectrum Protect Plus. Para instruções, consulte Registrando o Locatário do Office 365 com IBM Spectrum Protect Plus

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- Aplique uma política de acordo de nível de serviço (SLA). Para obter instruções, consulte [Criar políticas de backup](#).

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- Para fazer backup do e-mail, calendários, contatos e dados do Microsoft Office 365 no armazenamento em nuvem do OneDrive, consulte [Fazendo backup de dados do Office 365](#).
- Para restaurar dados do Office 365 de cópias de backup em servidores vSnap ou armazenamento remoto, consulte [Restaurando dados do Office 365](#).

Conectividade

Assegure-se de que os requisitos de conectividade a seguir sejam atendidos:

- O subsistema de protocolo de transferência de arquivos seguro (SFTP) para o Secure Shell (SSH) está ativado.
- O serviço do Secure Shell (SSH) está em execução na porta 22 no servidor host do proxy.
- Os firewalls são configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor host do proxy usando o SSH.
- O IBM Spectrum Protect Plus usa o protocolo do Network File System (NFS) para montar volumes de armazenamento para operações de backup e de restauração. Assegure-se de que o cliente NFS do Linux nativo esteja instalado no servidor host do proxy.
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Sistema de Nomes de Domínio (DNS) ou um endereço do protocolo da Internet (IP).
- Se os nomes do DNS forem usados, eles devem ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e pelo servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.
- Se o DNS não estiver disponível, você deve incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual IBM Spectrum Protect Plus usando a linha de comandos.

Portas

As portas a seguir são usadas pelos usuários dos agentes do IBM Spectrum Protect Plus.

Tabela 40. Portas de comunicação quando o destino é um usuário do agente IBM Spectrum Protect Plus				
Porta	Protocolo	Iniciador	Resposta	Descrição
22	Transmission Control Protocol (TCP)	Dispositivo virtual do IBM Spectrum Protect Plus ¹	Servidor host do proxy	Fornece acesso para solucionar problemas e manter servidores host do proxy remotos que estão executando componentes de aplicativos guest usando o protocolo SSH
¹ O dispositivo virtual IBM Spectrum Protect Plus contém os seguintes componentes de base: servidor IBM Spectrum Protect Plus, servidor vSnap e um proxy VADP, conforme descrito em Componentes do produto				

Tabela 41. Portas de comunicação quando o inicializador for um usuário do agente do IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
111	TCP	Servidor host do proxy	servidor vSnap	Permite que clientes do Open Network Computing (ONC) descubram portas para comunicações com servidores ONC
443	TCP	Servidor host do proxy	servidor vSnap	Porta que permite que o agente se comunique com IBM Spectrum Protect Plus para envio de alertas em caso de falhas de backup do log
2049	TCP	Servidor host do proxy	servidor vSnap	Usado para transferência de dados do NFS para e de servidores vSnap
20048	TCP	Servidor host do proxy	servidor vSnap	Monta sistemas de arquivos do vSnap em clientes como o proxy do VMware vStorage API for Data Protection (VADP), servidores de aplicativos e armazenamentos de dados de virtualização

Hardware

Tabela 42. Requisitos Mínimos de Hardware

System	Espaço em Disco	do NT
Hardware compatível com processadores quad-core suportados pelo sistema operacional	5 GB de espaço em disco disponível para arquivos temporários no tempo de execução	4 GB de Memória de Acesso Aleatório (RAM)

Requisitos de backup e restauração do banco de dados Oracle Server

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 [Nota técnica 304861](#).

Configuração

Versões do Aplicativo

Tabela 43. Matriz de cobertura para níveis do aplicativo suportados pelo IBM Spectrum Protect Plus					
IBM Spectrum Protect Plus	Oracle 11g R2*	Oracle 12c R1*	Oracle 12c R2*	Oracle 18c*	Oracle 19c*
V10.1.1	✓	✓	✓	--	--
V10.1.2	✓	✓	✓	--	--
V10.1.3	✓	✓	✓	✓	--
V10.1.4	✓	✓	✓	✓	--
V10.1.5	✓	✓	✓	✓	✓
V10.1.6	✓	✓	✓	✓	✓
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.					

Dica: Para bancos de dados multilocatários no Oracle 12c e mais recente, o IBM Spectrum Protect Plus suporta proteção e recuperação do banco de dados do contêiner, incluindo todos os bancos de dados plugáveis (PDBs) sob ele. A recuperação granular de PDBs específicos pode ser executada usando uma operação de recuperação de Restauração de Disco Instantâneo combinada com o Recovery Manager (RMAN).

Sistemas operacionais

Tabela 44. Matriz de cobertura para sistemas operacionais suportados no IBM PowerPC		
IBM Spectrum Protect Plus	IBM AIX 6.1 TL9*	IBM AIX 7.1*
V10.1.1	✓	✓
V10.1.2	✓	✓
V10.1.3	✓	✓
V10.1.4	✓	✓
V10.1.5	✓	✓
V10.1.6	✓	✓

Tabela 44. Matriz de cobertura para sistemas operacionais suportados no IBM PowerPC (continuação)

IBM Spectrum Protect Plus	IBM AIX 6.1 TL9*	IBM AIX 7.1*
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.		

Tabela 45. Matriz de cobertura para sistemas operacionais suportados no Linux® x86_64

IBM Spectrum Protect Plus	RHEL 6.5*	RHEL 7.0*	RHEL 8.0*	CentOS 6.5*	CentOS 7.0*	CentOS 8.0*	SLES 11.0 SP4*	SLES 12.0 SP1*	SLES 15.0*
V10.1.1	✓	✓	--	✓	✓	--	✓	✓	--
V10.1.2	✓	✓	--	✓	✓	--	✓	✓	--
V10.1.3	✓	✓	--	✓	✓	--	✓	✓	--
V10.1.4	✓	✓	--	✓	✓	--	✓	✓	✓
V10.1.5	✓	✓	--	✓	✓	--	✓	✓	✓
V10.1.6	✓	✓	✓	✓	✓	✓	✓	✓	✓
*A liberação base e os níveis de manutenção e modificação posteriores são suportados.									

Restrições

- 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 operações de recuperação do banco de dados Real Application Cluster (RAC) não têm reconhecimento de 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 multienlaceamento no momento do backup, o banco de dados restaurado é não multienlaceado. O banco de dados restaurado deve ser reconfigurado manualmente para usar multienlaceamento.
- 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.

Sistema de Arquivo de Rede (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.

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

Para o Direct NFS operar corretamente, o executável `oracle_home/bin/oradism` em cada diretório inicial do Oracle deve pertencer ao usuário raiz e ter privilégios **setuid**. Geralmente, o binário é pré-configurado pelo instalador do Oracle, mas em determinados sistemas, esse binário pode não ter os privilégios necessários. Execute os seguintes comandos para configurar os privilégios corretos:

- `chown root:oinstall oracle_home/bin/oradism`

em que `oinstall` especifica o grupo que possui a instalação e `oracle_home` especifica o diretório inicial do Oracle.

- `chmod 750 oracle_home/bin/oradism`

Descoberta de banco

IBM Spectrum Protect Plus descobre instalações e bancos de dados Oracle procurando os arquivos `/etc/orainst.loc` e `/etc/oratab` e a lista de processos do Oracle em execução. Se os arquivos não estiverem presentes em seu local padrão, o utilitário **locate** 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 a instâncias em execução e consultando os locais de seus arquivos de dados, arquivos de log e outros arquivos. 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 rastreamento de mudanças do bloco Oracle seja ativado em bancos de dados protegidos para executar com eficiência backups incrementais. Se o rastreamento de mudança de bloco ainda não estiver ativado, o IBM Spectrum Protect Plus o ativa automaticamente durante a tarefa de backup.

Para customizar o posicionamento do arquivo de rastreamento de mudança de bloco, você deve ativar manualmente o recurso de rastreamento de mudança de bloco antes de executar uma tarefa de backup associada. Se o recurso for ativado automaticamente pelo IBM Spectrum Protect Plus, serão utilizadas as seguintes regras para determinar a colocação do arquivo de rastreamento de mudança de blocos:

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

Software

- Os pacotes `bash` e **sudo** devem ser instalados. O pacote `sudo` deve ser versão 1.7.6p2 ou posterior. Execute **sudo -V** para verificar a versão.

Dica: Os pacotes necessários **bash** e **sudo** são incluídos nos sistemas operacionais Linux x86_64 suportados.

- Instale as correções e atualizações do Oracle Server mais recentes em seu ambiente.
- Assegure-se de que uma versão suportada do Linux x86_64 ou do Linux on Power Systems (little endian) esteja instalada. Assegure-se de que as correções e as atualizações mais recentes estejam instaladas.
- O International Components for Unicode (libicu) rpm-package deve ser instalado para a versão correspondente do seu sistema operacional.
- Assegure-se de que o tamanho do arquivo efetivo **ulimit -f** para o usuário do agente IBM Spectrum Protect Plus e o usuário da instância do Oracle esteja configurado como `unlimited`. Como alternativa, configure o valor para um valor suficientemente alto para permitir a cópia dos arquivos maiores de

banco de dados em suas tarefas de backup e de restauração. Se você alterar a configuração **ulimit**, reinicie a instância do Oracle para finalizar a configuração.

- Em um ambiente Linux, dependendo da sua versão ou distribuição, assegure-se de que o pacote do utilitário `util-linux-ng` ou `util-linux` do Linux seja atual.
- Para usuários do Red Hat Enterprise Linux e CentOS 6: para assegurar que o pacote `util-linux-ng` ou `util-linux` seja atual, execute o seguinte comando:

```
yum update package_name
```

Autenticação e Privilégios

Autenticação

- O Servidor Oracle deve ser registrado no IBM Spectrum Protect Plus usando um usuário do sistema operacional que exista no Oracle Server. O usuário é então chamado de *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.

Privilégios

Para usar um Oracle Server, o usuário do agente IBM Spectrum Protect Plus deve ter as permissões a seguir:

- Privilégios para executar comandos como root e como um usuário proprietário do software Oracle (por exemplo, `oracle` ou `grid`) usando **sudo**. Esses privilégios são necessários para tarefas, como descobrir layouts de armazenamento, montar e desmontar discos e gerenciar bancos de dados e Automatic Storage Management (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_KEE` 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 esses privilégios, o usuário do agente IBM Spectrum Protect Plus deve pertencer ao grupo de inventário do Oracle, geralmente denominado `oinstall`.

Para obter informações sobre a criação de um novo usuário com os privilégios necessários, consulte [“Configuração de amostra de um usuário do agente IBM Spectrum Protect Plus” na página 86](#).

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

Os comandos a seguir são exemplos para criação e configuração de um usuário do sistema operacional que o IBM Spectrum Protect Plus usa para efetuar login no Oracle Server. A sintaxe de comando pode variar dependendo do tipo e da versão do seu sistema operacional.

- Crie o usuário que é designado como o usuário do agente IBM Spectrum Protect Plus:

```
useradd -m sppagent
```

- Configure uma senha:

```
passwd sppagent_password
```

- Se estiver usando a autenticação baseada em chave, coloque a chave pública no diretório `/home/sppagent/.ssh/authorized_keys` ou o arquivo apropriado, dependendo da sua configuração

sshd, e assegure-se de que a propriedade e as permissões corretas estejam configuradas. Os comandos são estruturados conforme mostrado no exemplo a seguir:

```
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 do sistema operacional (OSDBA):

```
usermod -a -G oinstall, dba sppagent
```

- Se você planeja usar o ASM, inclua também o usuário no grupo OSASM:

```
usermod -a -G asmadmin sppagent
```

- Coloque as linhas a seguir no final do arquivo de configuração sudoers, geralmente /etc/sudoers. Se o arquivo sudoers existente estiver configurado para importar uma configuração a partir de outro diretório (por exemplo, /etc/sudoers.d), você também poderá 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
```

Pré-requisitos e operações

Pré-requisitos

Assegure-se de que os requisitos do [“Software”](#) na página 85, [“Conectividade”](#) na página 88 e [“Autenticação e Privilégios”](#) na página 86 sejam atendidos.

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- 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 funções usando a área de janela **Contas**. Para obter mais informações, consulte [Capítulo 18, “Gerenciando o acesso de”,](#) na página 517.
- Registre os provedores dos quais você deseja fazer backup. Para obter mais informações, consulte [“Incluindo um servidor de aplicativos Oracle”](#) na página 462.
- Configure uma política de acordo de nível de serviço (SLA). Para obter mais informações, consulte [“Criar políticas de backup”](#) na página 163.

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- Para assegurar que as permissões do sistema de arquivos sejam retidas corretamente quando o IBM Spectrum Protect Plus movimentar os dados do Oracle entre servidores, assegure-se de que os IDs do usuário e do grupo dos usuários do Oracle (por exemplo, oracle, oinstall, dba) estejam consistentes em todos os servidores. Para obter informações sobre os valores uid e gid, consulte a documentação do Oracle Database.
- Se uma tarefa de inventário do Oracle for executada ao mesmo tempo ou pouco depois de uma tarefa de backup do Oracle, poderão ocorrer erros de cópia por causa de montagens temporárias que são criadas durante a tarefa de backup. Para evitar esse problema, planeje as tarefas de inventário do Oracle para que elas não se sobreponham às tarefas de backup do Oracle.
- Evite configurar backup de log para um único Oracle Database usando várias tarefas de backup. Se um único Oracle Database for incluído em várias definições de tarefa com backup de log ativado, um backup de log de uma tarefa poderá truncar um log antes de ele ser submetido a backup pela próxima tarefa. Esse comportamento pode fazer com que as tarefas de restauração point-in-time falhem.
- Use uma tarefa de backup para fazer backup de ambientes Oracle com capturas instantâneas, conforme descrito em [“Fazendo Backup de Dados do Oracle”](#) na página 464.

- 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 definição de tarefa e cria um compartilhamento NFS. O agente IBM Spectrum Protect Plus monta então o compartilhamento no Oracle Server onde 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, conforme descrito em [“Restaurando dados do Oracle”](#) na página 467.
- Ao restaurar dados de um arquivo IBM Spectrum Protect, os arquivos são migrados inicialmente do armazenamento em fita para um conjunto temporário. Dependendo do tamanho dos arquivos a serem restaurados, esse processo pode levar várias horas.
- Se um Oracle Database for montado, mas não aberto durante uma tarefa de backup, o IBM Spectrum Protect Plus não pode determinar as configurações do banco de dados `tempfile` que estão relacionadas a `autoextendibility` e o 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 as configurações padrão: `AUTOEXTEND ON` e `MAXSIZE 32767M`. Após a conclusão da tarefa de restauração, é possível atualizar manualmente as configurações.

Backup de log

- O daemon **cron** deve ser ativado no servidor de aplicativos.
- O usuário do agente 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`.

Conectividade

Assegure-se de que os requisitos de conectividade a seguir sejam atendidos:

- O subsistema de protocolo de transferência de arquivos seguro (SFTP) para o Secure Shell (SSH) está ativado.
- O serviço SSH deve estar em execução na porta 22 no servidor host do proxy.
- Os firewalls são configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor host do proxy usando o SSH.
- O IBM Spectrum Protect Plus usa o protocolo do Network File System (NFS) para montar volumes de armazenamento para operações de backup e de restauração. Assegure-se de que o cliente NFS do Linux nativo esteja instalado no servidor host do proxy.
- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Domain Name System (DNS) ou um endereço do Internet Protocol (IP).
- Se os nomes DNS forem usados, eles devem ser resolvíveis pelo servidor de dispositivo virtual IBM Spectrum Protect Plus e pelo servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes DNS.
- Se o DNS não estiver disponível, você deverá incluir o servidor no arquivo `/etc/hosts` no dispositivo virtual do IBM Spectrum Protect Plus usando a linha de comandos.
- Os nós do Oracle RAC são registrados por seu IP físico ou nome. Não use um nome virtual ou Single Client Access Name (SCAN).

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus.

Tabela 46. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
22	Transmission Control Protocol (TCP)	Dispositivo virtual IBM Spectrum Protect Plus ¹	Oracle Server	Fornecer acesso para solucionar problemas e manter servidores host do proxy remotos executando componentes de aplicativos guest usando o protocolo SSH

¹ O dispositivo virtual do IBM Spectrum Protect Plus contém os componentes de base: o servidor IBM Spectrum Protect Plus, o servidor vSnap e um proxy do VADP, conforme descrito em “Componentes do Produto” na página 6.

Tabela 47. Portas de comunicação quando o inicializador for um usuário do agente IBM Spectrum Protect Plus

Porta	Protocolo	Iniciador	Resposta	Descrição
111	TCP	Oracle Server	servidor vSnap	Permite que clientes do Open Network Computing (ONC) descubram portas para comunicações com servidores ONC
443	TCP	Oracle Server	Dispositivo virtual IBM Spectrum Protect Plus ¹	Porta que permite que o agente se comunique com o IBM Spectrum Protect Plus para enviar alertas em caso de falhas de backup do log
2049	TCP	Oracle Server	servidor vSnap	Usado para transferência de dados do NFS para e de servidores vSnap
20048	TCP	Oracle Server	servidor vSnap	Monta sistemas de arquivos do vSnap em clientes como o proxy do VMware vStorage API for Data Protection (VADP), servidores de aplicativos e armazenamentos de dados de virtualização

Tabela 47. Portas de comunicação quando o inicializador for um usuário do agente IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
¹ O dispositivo virtual do IBM Spectrum Protect Plus contém os componentes de base: o servidor IBM Spectrum Protect Plus, o servidor vSnap e um proxy do VADP, conforme descrito em “Componentes do Produto” na página 6.				

Hardware

Tabela 48. Requisitos Mínimos de Hardware

System	Espaço em Disco
Hardware compatível que é suportado pelo sistema operacional e pelo Oracle Server	Um mínimo de 500 MB de espaço em disco para o produto ser instalado

Requisitos de backup e restauração do banco de dados Microsoft 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 [Nota técnica 304861](#).

Configuração

Versões do Aplicativo

Tabela 49. Matriz de cobertura para níveis do aplicativo suportados pelo IBM Spectrum Protect Plus

















































IBM Spectrum Protect Plus	Microsoft SQL Server 2008 R2 SP3* Standard e Enterprise Editions	Microsoft SQL Server 2012* Standard e Enterprise Editions	Microsoft SQL Server 2014* Standard e Enterprise Editions	Microsoft SQL Server 2016* Standard e Enterprise Editions	Microsoft SQL Server 2017* Standard e Enterprise Editions	Microsoft SQL Server 2019* Standard e Enterprise Editions
V10.1.1					 Início com V10.1.1 patch 1	--
V10.1.2						--
V10.1.3						--
V10.1.4						--

Tabela 49. Matriz de cobertura para níveis do aplicativo suportados pelo IBM Spectrum Protect Plus (continuação)

IBM Spectrum Protect Plus	Microsoft SQL Server 2008 R2 SP3* Standard e Enterprise Editions	Microsoft SQL Server 2012* Standard e Enterprise Editions	Microsoft SQL Server 2014* Standard e Enterprise Editions	Microsoft SQL Server 2016* Standard e Enterprise Editions	Microsoft SQL Server 2017* Standard e Enterprise Editions	Microsoft SQL Server 2019* Standard e Enterprise Editions
V10.1.5						 Início com V10.1.5 patch 1
V10.1.6						
* A liberação base e as atualizações acumulativas posteriores e os níveis de manutenção são suportados.						

Sistemas operacionais

Tabela 50. Matriz de cobertura para sistemas operacionais suportados no Windows x64

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Edições padrão e de data center	Microsoft Windows Server 2016* Edições padrão e de data center	Microsoft Windows Server 2019* Edições padrão e de data center
V10.1.1			--
V10.1.2			--
V10.1.3			
V10.1.4			
V10.1.5			
V10.1.6			
* A liberação base e os níveis de manutenção posteriores são suportados.			

Restrições

As seguintes restrições são aplicadas:

- O IBM Spectrum Protect Plus não suporta backup de log de modelos de recuperação simples.
- O failover de uma instância de cluster SQL durante operações de backup não é suportado.

- O caminho do arquivo de restauração do Serviço de Cópia de Sombra de Volume (VSS) é limitado a 256 ou menos caracteres. Se o caminho original exceder esse comprimento, considere o uso de um caminho de arquivo de restauração customizado para tarefas de restauração de produção para reduzir o comprimento.
- Devido a limitações da estrutura do VSS, espaços à esquerda, espaços à direita e caracteres não imprimíveis não devem ser usados em nomes de banco de dados. Para obter mais informações, consulte [Fazer backup de um banco de dados do SQL Server usando um aplicativo de backup do VSS pode falhar em alguns bancos de dados](#).
- Não é possível restaurar dados para um volume compactado do New Technology File System (NTFS) ou de tabela de alocação de arquivo (FAT) devido a restrições de banco de dados do SQL Server. Para obter mais informações, consulte [Descrição de suporte para bancos de dados SQL Server em volumes compactados](#).

Software

- Instale as correções e atualizações mais recentes do Microsoft SQL Server em seu ambiente.
- Instale uma versão suportada de um sistema operacional Windows de 64 bits em seu ambiente. Assegure-se de que as correções e as atualizações mais recentes estejam instaladas.

Autenticação e Privilégios

Autenticação

Registre cada Microsoft SQL Server com IBM Spectrum Protect Plus por nome ou endereço IP. Ao registrar um nó do cluster do SQL Server, registre cada nó por nome ou endereço IP.

Restrição: O endereço IP deve ser acessível por meio do servidor IBM Spectrum Protect Plus e por meio do servidor vSnap. Ambos os servidores devem ter um serviço Windows Remote Management (WinRM) que esteja atendendo na porta 5985. O nome completo do domínio deve ser resolvível e pode ser roteado do servidor IBM Spectrum Protect Plus e do servidor vSnap.

A identidade do usuário deve ter direitos suficientes para instalar e iniciar o IBM Spectrum Protect Plus Tools Service no nó. Essas permissões incluem os direitos Log on as a service e Log on as batch job na política de segurança local. Para obter mais informações, consulte o artigo Microsoft: [Incluir o direito Efetuar logon como um serviço em uma conta](#)

Se o SQL Server estiver conectado a um domínio, a identidade do usuário segue o formato padrão domain \Name. Se o usuário for um administrador local, a identidade do usuário corresponde ao nome do administrador local.

Autenticação do Kerberos

A autenticação baseada em Kerberos pode ser ativada especificando um arquivo de configuração no dispositivo virtual IBM Spectrum Protect Plus. As configurações substituem o protocolo padrão do Windows NT LAN Manager (NTLM).

Somente para autenticação baseada em Kerberos, a identidade do usuário deve ser especificada no formato username@FQDN. O 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 que é especificado pelo nome completo do domínio.

Privilégios

Para usar um Microsoft SQL Server, um usuário do agente IBM Spectrum Protect Plus deve ter as permissões a seguir:

- Permissões public e sysadmin do Microsoft SQL Server
- Permissões de administração local do Windows, que são requeridas pela estrutura do VSS, e acesso de volume e disco
- Permissões para acessar recursos de cluster em um ambiente SQL Server Always On e SQL Server failover clustering instance (FCI)

Cada host do Microsoft SQL Server pode usar uma conta de usuário específica para acessar os recursos daquela instância do SQL Server.

A estrutura baseada em SQL Server Virtual Device Interface (VDI) é usada para interagir com bancos de dados SQL Server e para operações de backup de log e restauração. Uma conexão VDI requer permissões sysadmin do Microsoft 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 Microsoft: [As operações de backup e restauração de VDI do SQL Server requerem privilégios Sysadmin](#)

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

O Planejador de Tarefas Windows é usado para planejar backups de log. Dependendo do ambiente, os usuários podem receber o seguinte erro:

Uma sessão de logon especificada não existe. Talvez ela já tenha sido finalizada.

Esse comportamento ocorre quando uma configuração de política do grupo de acesso à rede está ativada. Para obter instruções sobre a desativação da configuração, consulte o artigo de Suporte Microsoft: [Erro do Planejador de Tarefas "Uma sessão de logon especificada não existe"](#)

Objeto de Política de Grupo

Para a configuração **Segurança de rede: política de nível de autenticação do LAN Manager** em **Configuração do Computador > Configurações do Windows > Configurações de Segurança > Políticas Locais > Opções de Segurança**, especifique uma das opções a seguir:

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

A opção **Enviar apenas a resposta NTLM** não é compatível com a versão do vSnap Common Internet File System (CIFS) e do Bloco de Mensagens do Servidor (SMB) e pode causar problemas de autenticação do CIFS.

É possível especificar a configuração de Objeto de política de grupo (GPO) navegando para:

- **Configuração do computador > Políticas > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança > Segurança de rede: NTLM restrito: tráfego de NTLM recebido**

Ou este

- **Configuração do computador > Políticas > Configurações do Windows > Configurações de segurança > Políticas locais > Opções de segurança > Segurança de rede: NTLM restrito: tráfego de NTLM de saída**

Em seguida, escolha uma das opções a seguir:

- **Permitir Tudo**
- **Permitir todas as contas**

Pré-requisitos e operações

Pré-requisitos

Assegure-se de que os requisitos do [“Software”](#) na página 92, [“Conectividade”](#) na página 96 e [“Autenticação e Privilégios”](#) na página 92 sejam atendidos.

Os pré-requisitos a seguir devem ser atendidos antes de você iniciar a proteção de seus recursos:

- Uma rota Internet Small Computer Interface (iSCSI) deve ser ativada entre o sistema Microsoft SQL Server e o servidor vSnap. Para obter mais informações, consulte [Microsoft iSCSI Initiator Step-by-Step Guide](#).
- O caminho binário do PowerShell Windows deve ser configurado na variável de ambiente %PATH%.
- Se você planeja fazer backup de bancos de dados que foram restaurados no modo de teste, use a preferência global para limitar o tamanho dos volumes de destino de backup para menos de 64 TB. Você deve configurar essa preferência global antes de executar o primeiro backup para o acordo de nível de serviço (SLA) que protege os bancos de dados. Se o tamanho dos volumes de destino de backup for 64 TB ou mais, a tarefa de backup falhará.

Operações

Antes de você iniciar uma operação de backup ou de restauração:

- Registre os Servidores SQL do quais você deseja fazer backup. Quando um servidor de aplicativos SQL Server 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. O inventário é necessário para tarefas de backup e restauração e execução de relatórios. Para obter instruções, consulte [“Incluindo um servidor de aplicativos SQL Server”](#) na página 475.
- Configure políticas de acordo de nível de serviço (SLA). Para obter instruções, consulte [“Criar políticas de backup”](#) na página 163.
- 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 aos recursos e às operações de backup e restauração usando a área de janela **Contas**. Para obter instruções, consulte [Capítulo 18, “Gerenciando o acesso de”,](#) na página 517.
- Antes de configurar e executar tarefas de backup SQL, configure as definições de armazenamento de cópia de sombra para os volumes em que os bancos de dados SQL estão localizados. Essa configuração é feita uma vez para cada volume. Se novos bancos de dados forem incluídos na tarefa, a configuração deverá ser configurada para quaisquer novos volumes que contenham bancos de dados SQL. No Windows Explorer, clique com o botão direito do mouse no volume de origem e clique na guia **Cópias de Sombra**. Configure o valor **Tamanho Máximo** para **Nenhum Limite** ou um tamanho razoável com base no tamanho do volume de origem e nas atividades de entrada / saída (E/S) e, em seguida, clique em **OK**. A área de armazenamento de cópia de sombra deve estar em um mesmo volume ou outro volume disponível durante uma tarefa de backup.
- 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 número máximo do valor 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 valor padrão para o máximo de encadeamentos do trabalhador pode não ser suficiente para fazer backup de todos os bancos de dados e a tarefa falha. Para obter instruções sobre como aumentar a opção máxima de encadeamentos do trabalhador, consulte [Configurar a opção de configuração do servidor máximo de encadeamentos do trabalhador](#).
- 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](#).

Revise as informações a seguir sobre a criação de tarefas de backup e de restauração:

- Use uma tarefa de backup para fazer backup de ambientes SQL Server com capturas instantâneas. Para obter instruções, consulte [“Fazendo Backup dos Dados do SQL Server”](#) na página 477.
- O IBM Spectrum Protect Plus suporta backups de banco de dados e backups do log de transações. O nome do produto é preenchido no msdb . dbo . backupset para registros criados por backups iniciados a partir de IBM Spectrum Protect Plus.

- 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. O IBM Spectrum Protect Plus cataloga e rastreia todas as instâncias clonadas, conforme descrito em [“Restaurando os Dados do SQL Server”](#) na página 481.
- 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.
- 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.
- Ao restaurar dados de um archive do IBM Spectrum Protect, os arquivos são migrados inicialmente do armazenamento em fita para um conjunto de armazenamento temporário. Dependendo do tamanho da restauração, esse processo pode levar várias horas.
- 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 banco de dados secundário recebe um valor inicial do SQL Server em ambientes em que a atribuição automática de valor inicial é suportada (Microsoft SQL Server 2016 e posterior). 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 atribuição automática de valor inicial não for suportada ou não estiver ativada, você deve iniciar uma tarefa de restauração secundária a partir do ponto de restauração com a diferença de Números de Sequência de Log (LSN) mais curta da instância primária. 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 secundária é concluída no estado RESTORE e você deve emitir o comando T-SQL para incluir o banco de dados no grupo de destino. Para obter mais informações, consulte [Transact-Referência de SQL \(Mecanismo de Banco de Dados\)](#).

Processamento de transações on-line (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 Microsoft SQL Server 2014 e posterior. Os requisitos e limitações a seguir se aplicam ao uso do OLTP na Memória:

- O caminho do arquivo de restauração é limitado a 256 ou menos 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 a recursos de restauração do Serviço de Cópia de Sombra de Volume (VSS) e do Microsoft SQL Server.

Configurando grupos de disponibilidade Always On

Configure a instância preferencial para operações de backup usando o Microsoft 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. Em seguida, selecione **Propriedades**.
3. Na caixa de diálogo **Propriedades do grupo de disponibilidade**, selecione **Preferências de backup**.
4. Na área de janela **Onde devem ocorrer backups**, selecione qualquer opção.

Quando uma réplica secundária é preferencial, e mais de uma réplica secundária está disponível, o executor de tarefa IBM Spectrum Protect Plus seleciona a primeira réplica secundária na lista preferencial relatada pelo agente do IBM Spectrum Protect Plus SQL Server.

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

A opção **Sem Recuperação** não suporta operações de restauração do modo de produção para grupos de disponibilidade SQL Always On.

Backups incrementais

O IBM Spectrum Protect Plus usa a tecnologia de diário de mudanças update sequence number (USN) para executar backups incrementais em um ambiente Microsoft 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.

Para ativar o rastreamento do intervalo de gravação, o ambiente do sistema deve atender aos requisitos a seguir:

- 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 SMB 3.0
- Transparent Failover (TFO) do SMB
- SMB 3.0 com compartilhamentos de arquivos 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 é detectado, o espaço alocado dobra de tamanho, atingindo um máximo de 2 GB.

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. Se o espaço livre no volume de origem for menor que 100 MB, o agente do Microsoft SQL Server verifica o espaço de volume de origem e faz a operação de backup falhar. 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. Essa condição pode ocorrer quando o log atingir o tamanho máximo, quando o registro no diário estiver desativado ou quando o ID USN catalogado for alterado.
- O tamanho do arquivo é menor que ou igual ao tamanho do limite de rastreamento, que por padrão é 1 MB.
- Um arquivo é incluído após uma tarefa de backup anterior.

Backups de log

Para assegurar que o backup de log do SQL funcione corretamente, talvez você tenha que atualizar as configurações do Windows Group Policy Object. Para obter mais informações, consulte [Group Policy Object](#).

Conectividade

Assegure-se de que os requisitos de conectividade a seguir sejam atendidos:

- O adaptador de rede usado para a conexão deve ser configurado como um cliente para o Microsoft Networks.
- O serviço do Microsoft Windows Remote Management (WinRM) deve estar em execução.
- Os firewalls devem ser configurados para permitir que o IBM Spectrum Protect Plus se conecte ao servidor usando o WinRM.
- O endereço IP da máquina que você registra deve ser acessível por meio do servidor IBM Spectrum Protect Plus e por meio do servidor vSnap. O SQL Server deve ter um serviço WinRM que esteja atendendo na porta 5985.

- Todos os servidores, proxies, aplicativos e hypervisors que são incluídos no ambiente do IBM Spectrum Protect Plus devem ser registrados usando um nome do Domain Name System (DNS) ou um endereço do Internet Protocol (IP).
- Se os nomes do DNS forem usados, eles deverão ser resolvíveis sobre a rede pelo servidor de dispositivo virtual do IBM Spectrum Protect Plus e por meio do servidor vSnap. Todos os componentes do IBM Spectrum Protect Plus também devem ser resolvíveis por seus nomes do DNS.

Portas

As portas a seguir são usadas pelos usuários do agente do IBM Spectrum Protect Plus.

<i>Tabela 51. Portas de comunicação quando o destino for um agente do IBM Spectrum Protect Plus</i>				
Porta	Protocolo	Iniciador	Resposta	Descrição
5985	Transmission Control Protocol (TCP)	IBM Spectrum Protect Plus dispositivo virtual ¹	Microsoft SQL Server	Fornecer acesso ao serviço do Microsoft WinRm para servidores baseados no Windows
5986	TCP	IBM Spectrum Protect Plus dispositivo virtual ¹	Microsoft SQL Server	Fornecer acesso ao serviço do Microsoft WinRm para servidores baseados no Windows
¹ O dispositivo virtual do IBM Spectrum Protect Plus contém os componentes de base: o servidor IBM Spectrum Protect Plus, o servidor vSnap e um proxy do VADP, conforme descrito em Componentes do produto .				

<i>Tabela 52. Portas de comunicação quando o inicializador for um usuário do agente IBM Spectrum Protect Plus</i>				
Porta	Protocolo	Iniciador	Resposta	Descrição
3260 O inicializador iSCSI é necessário nesse nó.	TCP	Microsoft SQL Server	servidor vSnap	A porta de destino vSnap do serviço Microsoft iSCSI Initiator port que é usada para montagem de LUNS para operações de backup e recuperação
443	TCP	Agente Microsoft SQL Server	IBM Spectrum Protect Plus dispositivo virtual ¹	Porta que permite que o agente se comunique com o IBM Spectrum Protect Plus para enviar alertas em caso de falhas de backup do log

Tabela 52. Portas de comunicação quando o inicializador for um usuário do agente IBM Spectrum Protect Plus (continuação)

Porta	Protocolo	Iniciador	Resposta	Descrição
445	TCP	Agente Microsoft SQL Server	servidor vSnap	Fornecer a porta de destino do SMB ou do CIFS do servidor vSnap que é usada para montar compartilhamentos do sistema de arquivos para operações de backup e recuperação do log de transações

¹ O dispositivo virtual do IBM Spectrum Protect Plus contém os componentes de base: o servidor IBM Spectrum Protect Plus, o servidor vSnap e um proxy do VADP, conforme descrito em [Componentes do produto](#).

Atualização de portas

- Para o Microsoft SQL Server, a porta 443 está disponível no IBM Spectrum Protect Plus V10.1.4 e mais recente.
- Em versões anteriores, as portas 137, 138 e 139 no servidor vSnap foram usadas por agentes de aplicativo que usam o SMBv1. Iniciando com o IBM Spectrum Protect Plus V10.1.6, o protocolo do SMBv1 não é usado. Todos os agentes usam o SMBv2 ou mais recente, que não requer as portas 137, 138 ou 139.

Hardware

Tabela 53. Requisitos Mínimos de Hardware

System	Espaço em Disco
Hardware compatível que é suportado pelo sistema operacional e Microsoft SQL Server	Um mínimo de 500 MB de espaço em disco para o produto a ser instalado

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 5693313](#).

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 173](#)

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 99](#)

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 101](#)

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 um servidor vSnap” na página 109](#)

Ao implementar um dispositivo IBM Spectrum Protect Plus, um servidor vSnap é instalado automaticamente. Você deve ter pelo menos um servidor vSnap instalado como parte de seu ambiente do IBM Spectrum Protect Plus. Este servidor é o destino do backup primário. Em ambientes corporativos maiores, podem ser necessários servidores vSnap adicionais. Os Blueprints ajudarão a determinar quantos servidores vSnap são necessários.

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 23](#) e [“Requisitos de restauração e backup do hypervisor \(Microsoft Hyper-V e VMware\) e da instância da nuvem \(Amazon EC2\)” na página 40](#).
- Faça o download do arquivo de instalação do modelo de dispositivo virtual `<part_number>.ova` a partir do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [Nota técnica 5693313](#).
- 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 103](#).

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.

Nota: O dispositivo do IBM Spectrum Protect Plus e do vSnap é uma instalação do sistema fechado e do antivírus (AV) que não é suportada em implementações virtuais ou físicas.

Procedimento

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

1. Implemente o IBM Spectrum Protect Plus. Usando o vSphere Client (HTML5) ou o vSphere Web Client (FLEX), a partir do menu **Ações**, clique em **Implementar Modelo de OVF**.
2. Especifique o local do arquivo `<part_number>.ova` e selecione-o. Clique em **Avançar**.
3. 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**.
4. Selecione um recurso de cálculo de destino apropriado. Clique em **Avançar**.
5. Revise os detalhes do modelo. Clique em **Avançar**.

Importante: Se você estiver usando o vSphere Web Client (FLEX), verifique se `disk.enableUUID = true` aparece na **Configuração Extra**. Se esse não for o caso, ou se você estiver usando o vSphere Client (HTML5), prossiga com as etapas de instalação e ative esta opção do vSphere Web Client posteriormente.

6. Leia 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**.
7. 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**.
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. Insira os valores de propriedade para o dispositivo virtual: Hostname, DNS, Default Gateway, Domain, Network IP Address e Network Prefix. 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: 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 104 .
Inicie IBM Spectrum Protect Plus a partir de um navegador da web suportado.	Consulte “Inicie o IBM Spectrum Protect Plus” na página 161 .

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 23](#) e [“Requisitos de restauração e backup do hypervisor \(Microsoft Hyper-V e VMware\) e da instância da nuvem \(Amazon EC2\)” na página 40](#).
- Faça o download do arquivo de instalação `<part_number>.exe` a partir do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [Nota técnica 5693313](#).
- 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.

Nota: O dispositivo do IBM Spectrum Protect Plus e do vSnap é uma instalação do sistema fechado e do antivírus (AV) que não é suportada em implementações virtuais ou físicas.

Procedimento

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

1. Copie o arquivo `<part_number>.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 de navegação, clique em **Hardware > Controlador IDE 0 > 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 12 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 103.

Importante: As máquinas virtuais IBM Spectrum Protect Plus ou vSnap que são implantadas usando o armazenamento em cluster de failover do Hyper-V devem ser configuradas com um endereço de

controle de acesso à mídia (MAC) estático para cada adaptador de rede virtual. Se um endereço MAC dinâmico for usado, a configuração de rede do Linux pode ser perdida após o failover porque um novo endereço MAC é designado ao adaptador de rede virtual. O endereço MAC pode ser configurado através da edição das configurações da máquina virtual no Hyper-V Manager ou Failover Cluster Manage. Garantir que cada adaptador de rede virtual receba um endereço MAC estático evitará a perda da configuração da rede.

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 104.
Inicie IBM Spectrum Protect Plus a partir de um navegador da web suportado.	Consulte “Inicie o IBM Spectrum Protect Plus” na página 161.

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-SysXyz`. É solicitado que mude esta senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161.](#)
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 99](#)

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 101](#)

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.

A aplicação de uma chave de produto válida usando o procedimento abaixo ativará os recursos do IBM Spectrum Protect Plus indefinidamente.

Procedimento

Nota: Quando um backup de catálogo de um servidor IBM Spectrum Protect Plus que está usando uma licença de avaliação durante o período de avaliação for restaurado para outro servidor IBM Spectrum Protect Plus também usando uma licença de teste no período de avaliação, a contagem de dias restante da licença de avaliação do servidor de origem de backup do catálogo ainda se aplicará. Isso não se aplica às licenças de produção com chaves de produtos válidas.

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-SysXyz`.

É solicitado que mude esta senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).

3. Clique em **Gerenciamento de Licença**.
4. Clique no botão **Atualizar Licença** e, em seguida, **Escolher Arquivo** para navegar na chave do produto em seu computador.
5. Clique em **Fazer Upload de uma Nova Licença**.
6. Quando o arquivo de licença tiver sido transferido por upload, 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 161 .

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

Use os comandos a seguir para abrir portas em servidores proxy remoto VADP 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 do 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 o tráfego TCP de entrada a partir 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 sub-rede externa **<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
```

Instalando utilitários de inicializadores iSCSI

Você deve instalar os utilitários Internet Small Computer System Interface (iSCSI) se os dispositivos de armazenamento montados por iSCSI estiverem conectados diretamente ao dispositivo IBM Spectrum Protect Plus ou a um servidor vSnap. Depois que os utilitários inicializadores do iSCSI são instalados, os dispositivos de armazenamento montados por iSCSI podem ser conectados ao dispositivo ou ao servidor no qual o pacote está instalado.

Sobre Esta Tarefa

Os utilitários inicializadores iSCSI podem ser instalados no dispositivo IBM Spectrum Protect Plus ou em um servidor vSnap. Os utilitários inicializadores iSCSI são entregues juntamente com IBM Spectrum Protect Plus, mas não são instalados automaticamente. Para instalar os utilitários, siga o procedimento.

Procedimento

1. Efetue login no dispositivo ou no servidor que deve ser conectado diretamente ao armazenamento montado pelo iSCSI.
 - Para o dispositivo IBM Spectrum Protect Plus, use o protocolo Secure Shell (SSH) e se autentique-se com as credenciais administrativas apropriadas.
 - Para um servidor vSnap, use SSH ou acesse o servidor diretamente e autentique-se com as credenciais administrativas apropriadas.
2. Instale os utilitários inicializadores iSCSI executando o seguinte comando:


```
sudo /usr/bin/yum --disablerepo=* --enablerepo=base,updates install iscsi-initiator-utils
```

Capítulo 3. Instalando 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. O servidor vSnap integrado deve ser utilizado apenas para fins de demonstração ou de teste e não utilizado em um ambiente de produção. Pelo menos um servidor vSnap deve ser implementado em seu ambiente.

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 um servidor vSnap

Ao implementar um dispositivo IBM Spectrum Protect Plus, um servidor vSnap é instalado automaticamente. Você deve ter pelo menos um servidor vSnap instalado como parte de seu ambiente do IBM Spectrum Protect Plus. Este servidor é o destino do backup primário. Em ambientes corporativos maiores, podem ser necessários servidores vSnap adicionais. Os Blueprints ajudarão a determinar quantos servidores vSnap são necessários.

Antes de Iniciar

Execute as seguintes etapas:

1. Revise os requisitos do sistema vSnap em “Requisitos do Componente ” na página 23.
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 mais informações sobre o download de arquivos e outras informações úteis, consulte a página de suporte a seguir <https://www.ibm.com/support/pages/node/567387>.

Nota: O dispositivo do IBM Spectrum Protect Plus e do vSnap é uma instalação do sistema fechado e do antivírus (AV) que não é suportada em implementações virtuais ou físicas.

Importante: Os componentes do IBM Spectrum Protect Plus, incluindo o vSnap, não devem ser instalados na mesma máquina, física ou virtual, como o IBM Spectrum Protect Server.

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 “[Instalação física do servidor vSnap](#)” na [página 31](#) 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 alterar o modo SELinux para Permissivo:

```
SELINUX=permissive
```

3. Emita o `setenforce 0` para aplicar a configuração imediatamente sem precisar reiniciar:

```
$ setenforce 0
```

4. Faça o download do arquivo de instalação `<part_number>.run` do vSnap a partir do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [Nota técnica 5693313](#).

5. Crie o executável do arquivo e, em seguida, execute o executável.

```
$ chmod +x <part_number>.run
```

6. Execute o executável. Os pacotes do vSnap são instalados, além de todos os componentes necessários.

```
$ ./<part_number>.run
```

Como alternativa, instalações não interativas ou atualizações do vSnap podem ser iniciadas usando a opção `noprompt`. Quando esta opção for usada, o instalador do vSnap ignorará o prompt para respostas e assumirá uma resposta "sim" para os prompts a seguir:

- Contrato de licença
- Instalação ou atualização do kernel
- Reinicializar no término da instalação ou atualizar, se necessário

Para usar a opção `noprompt`, emita o comando a seguir. Observe o espaço deliberado tanto antes quanto depois dos traços duplos:

```
$ sudo ./<part_number>.run -- noprompt
```

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 Capítulo 4, “Gerenciando servidores vSnap” , na página 115 .

Instalando um servidor vSnap virtual em um ambiente VMware

Para instalar um servidor vSnap virtual em um ambiente VMware, implemente um modelo de Open Virtualization Format (OVF). Isso cria uma máquina que contém o servidor vSnap.

Antes de Iniciar

Para facilitar a administração de rede, use um endereço IP estático da máquina virtual. Designe o endereço usando a ferramenta NetworkManager Text User Interface (nmtui).

Para obter instruções, consulte “[Designando um endereço IP estático](#)” na [página 103](#). Trabalhe com o administrador da rede ao configurar propriedades da rede.

Procedimento

1. Faça o download do arquivo de modelo do servidor `<part_number>.ova` do vSnap a partir do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [Nota técnica 5693313](#).
2. Implemente o servidor vSnap. Usando o vSphere Client (HTML5) ou o vSphere Web Client (FLEX), clique no menu **Ações** e, em seguida, clique em **Implementar Modelo OVF**.
3. Especifique o local do arquivo `<part_number>.ova` e selecione-o. Clique em **Avançar**.
4. 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**.
5. Selecione um recurso de cálculo de destino apropriado. Clique em **Avançar**.
6. Revise os detalhes do modelo. Clique em **Avançar**.
7. Leia 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 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**.
9. 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**.
10. 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.

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: É importante manter a VM ligada.

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 Capítulo 4, “Gerenciando servidores vSnap”, na página 115.
Para uma administração de rede mais fácil, designe um endereço IP estático da máquina virtual. Use a ferramenta NetworkManager Text User Interface (nmtui) para designar o endereço IP.	Para obter instruções, consulte “Designando um endereço IP estático” na página 103. Trabalhe com o administrador de rede ao configurar as propriedades de rede.

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 o download do arquivo de instalação <part_number>.exe do vSnap a partir do Passport Advantage Online. Para obter informações sobre como fazer download de arquivos, consulte [Nota técnica 5693313](#).
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 103.

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 Capítulo 4, “Gerenciando servidores vSnap”, na página 115.

Desinstalando um servidor vSnap

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

Antes de Iniciar

Ao excluir permanentemente o servidor vSnap, você deve limpar o servidor IBM Spectrum Protect Plus. Os itens que devem ser limpos nesse caso são os seguintes:

- Registros de backups que foram armazenados no servidor vSnap.
- Relacionamentos de replicação para outros servidores vSnap.
- Certifique-se de que nenhuma tarefa use políticas de SLA que definem o servidor vSnap como um local de backup.

Para visualizar as políticas de SLA 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**. Você deve cancelar o registro do servidor vSnap a partir do servidor IBM Spectrum Protect Plus. Consulte [“Cancelando o registro de um servidor vSnap” na página 116](#) para obter informações adicionais.



Atenção: A desinstalação de um servidor vSnap pode resultar em perda de dados.

Procedimento

1. Efetue login no console do servidor vSnap com o ID do usuário serveradmin. A senha inicial é sppDP758-SysXyz. É solicitado que mude esta senha durante o primeiro login. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).

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 129](#).

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 Hyper-V, exclua o dispositivo IBM Spectrum Protect Plus 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. Gerenciando servidores vSnap

Para ativar tarefas de backup e restauração, o IBM Spectrum Protect Plus requer pelo menos um servidor vSnap. O servidor vSnap é seu próprio dispositivo, implementado virtualmente ou instalado fisicamente em um sistema que atenda aos requisitos mínimos. Cada servidor vSnap no ambiente deve ser registrado no IBM Spectrum Protect Plus para ser reconhecido. O servidor vSnap que está registrado no site Demo que é incluído com o IBM Spectrum Protect Plus deve ser usado apenas para propósitos de teste e demonstração, e nunca deve ser utilizado como um destino de backup em um ambiente de produção.

Registrando 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 e registrar um servidor vSnap como um provedor de armazenamento de backup, você pode optar por configurar e administrar determinados aspectos do vSnap, como configuração de rede ou gerenciamento do conjunto de armazenamento. Para obter mais informações, consulte [“Configurando opções de armazenamento de backup”](#) na página 118.

Se o servidor vSnap também será registrado como um proxy do VADP, a conta incluída no campo **Propriedades de armazenamento** para o vSnap deverá ter privilégios **sudo** para que o registro de proxy do VADP tenha sucesso. Para obter mais informações, consulte [“Tipos de Permissão”](#) na página 523.

Procedimento

Para registrar um servidor vSnap como um dispositivo de armazenamento de backup, conclua as etapas a seguir:

1. Efetue logon no console do servidor vSnap com o ID do usuário `serveradmin`. A senha inicial é `sppDP758-SysXyz`.
É solicitado que mude esta senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus”](#) na página 161.
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 115.

Password

Insira a senha para o usuário.

7. Clique **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 “ Iniciando o servidor vSnap ” na página 126.
Expandir o conjunto de armazenamentos vSnap.	Consulte “ Configurando parceiros de armazenamento de backup ” na página 120.
Se necessário, configure e administre determinados aspectos do vSnap, como configuração de rede ou gerenciamento do conjunto de armazenamentos.	Consulte “ Configurando opções de armazenamento de backup ” na página 118

Tarefas relacionadas

“[Inicie o IBM Spectrum Protect Plus](#)” na página 161


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**.

Cancelando o registro de um servidor vSnap

Se necessário, é possível cancelar o registro de um servidor vSnap que não é mais usado em seu ambiente IBM Spectrum Protect Plus.

Antes de Iniciar

Quando um servidor vSnap tem seu registro cancelado, todos os pontos de recuperação que estão associados ao servidor vSnap são limpos do IBM Spectrum Protect Plus durante a próxima tarefa de manutenção.



Atenção: Cancelar o registro de um servidor vSnap pode resultar em perda de dados.

Antes de cancelar o registro de um servidor vSnap, revise os cenários para determinar se o cancelamento do registro é apropriado ou se outra ação deve ser tomada.

Cenário 1: o servidor vSnap está temporariamente inativo devido a problemas de armazenamento ou de rede.

- Não cancele o registro do servidor vSnap. Se você cancelar o registro do servidor vSnap, os pontos de recuperação que estiverem associados ao servidor serão limpos e os backups serão rebaseados.
- Conclua a manutenção de armazenamento ou rede necessária para deixar o servidor vSnap on-line novamente.

Cenário 2: o servidor vSnap recebe um novo nome de host ou endereço IP.

- Não cancele o registro do servidor vSnap. Se você cancelar o registro do servidor vSnap, os pontos de recuperação que estiverem associados ao servidor serão limpos e os backups serão rebaseados.
- Edite as configurações para o servidor vSnap para especificar o novo nome do host ou endereço IP. Para editar as configurações para um servidor vSnap, siga as instruções [“Editando Configurações para um Servidor vSnap” na página 116.](#)

Cenário 3: o servidor vSnap não está em uso, e não há planos para reutilizá-lo.

- Cancele o registro do servidor vSnap e execute uma tarefa de manutenção para assegurar que os pontos de recuperação que estão associados ao servidor vSnap sejam limpos do IBM Spectrum Protect Plus.
 - Os backups incrementais dos dados que estavam presentes no servidor vSnap não serão mais possíveis.
 - A recuperação de dados que estavam presentes no servidor vSnap não será mais possível.
- As execuções subsequentes de tarefas de backup criarão automaticamente novos volumes em outro servidor vSnap no mesmo site e executarão novos backups de base.

Cenário 4: o conjunto vSnap está perdido e você deseja construir um novo conjunto no mesmo servidor vSnap.


1. Cancele o registro do servidor vSnap e execute uma tarefa de manutenção para assegurar que os pontos de recuperação que estão associados ao antigo conjunto vSnap sejam limpos do IBM Spectrum Protect Plus.
 - Os backups incrementais dos dados que estavam presentes no conjunto antigo não serão mais possíveis.
 - A recuperação de dados que estavam presentes no conjunto antigo não será mais possível.
2. No servidor vSnap, crie um conjunto.
3. Inclua o servidor vSnap de volta em IBM Spectrum Protect Plus. Para incluir um servidor vSnap em IBM Spectrum Protect Plus, consulte [“Registrando um servidor vSnap como um provedor de armazenamento de backup” na página 115.](#)
 - As execuções subsequentes de tarefas de backup criarão volumes automaticamente neste ou em outro servidor vSnap no mesmo site e executarão novos backups de base.

Cenário 5: o conjunto vSnap ou servidor está perdido e você pretende repará-lo. Isso pode ser feito replicando dados de um servidor de replicação vSnap.

- Não cancele o registro do servidor vSnap a partir do IBM Spectrum Protect Plus. O processo de exclusão fará com que os backups sejam rebaseados.
- Substitua o servidor vSnap. Para obter informações sobre a substituição de um servidor vSnap primário com falha, consulte esta seção [“Resolução de problemas de servidores vSnap” na página 136.](#)

Procedimento

Para cancelar o registro de um servidor vSnap, conclua as etapas a seguir:

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. Confirme a remoção do servidor vSnap, inserindo o código na caixa de texto. Clique em **DELETE** para excluir o servidor de IBM Spectrum Protect Plus.

Configurando opções de armazenamento de backup


É possível configurar opções adicionais relacionadas ao armazenamento para seus hosts de armazenamento de backup primário e secundário.

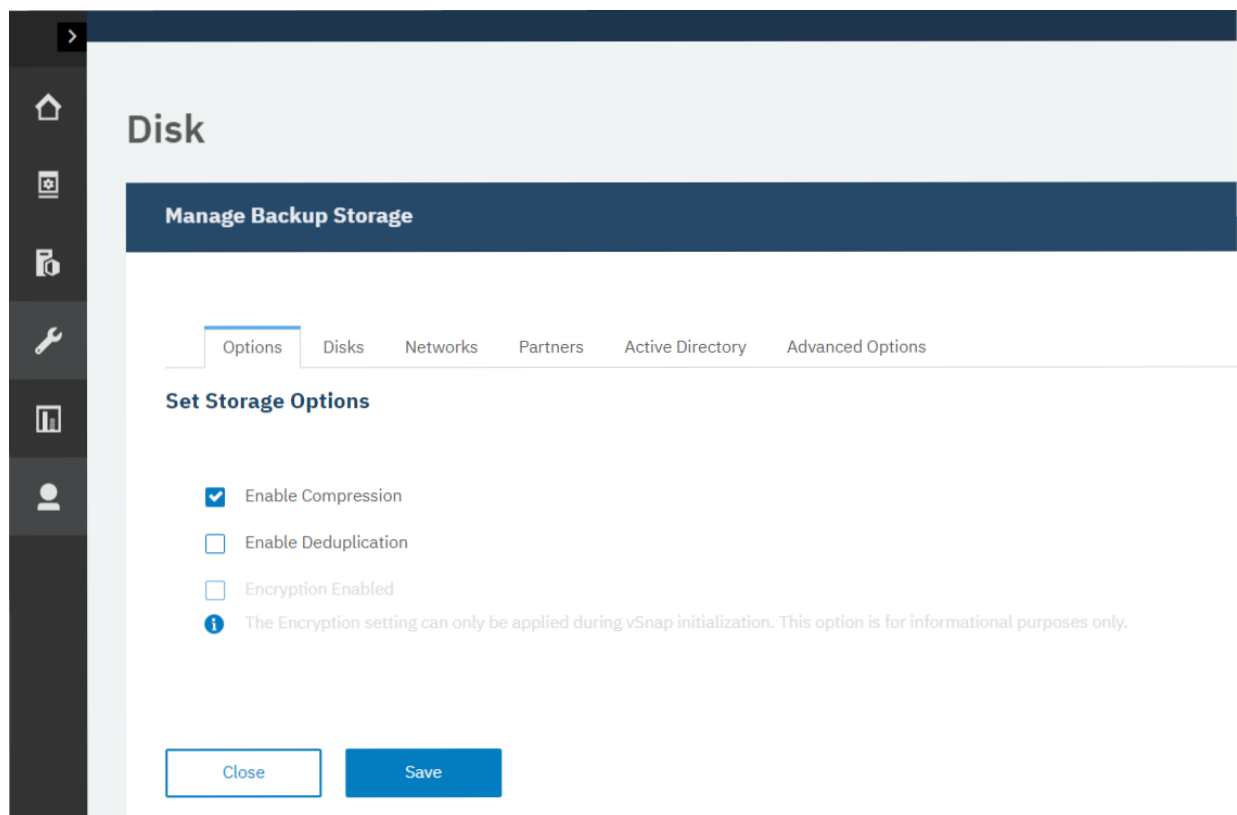
Procedimento

Para configurar opções de armazenamento de backup para seus discos registrados, conclua as etapas a seguir:

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

A tabela **Armazenamento em Disco** lista o nome do host de sites primários e secundários com a versão e o uso da capacidade.

2. Na área de janela **Armazenamento em Disco**, clique no ícone de configurações  que está associado ao disco que você deseja atualizar.
3. Selecione a partir das opções de armazenamento, conforme mostrado.



Ativar Compactação: selecione esta opção para compactar cada bloco de entrada de dados usando um algoritmo de compactação antes de os dados serem gravados no conjunto de armazenamentos. A compactação consome uma quantidade moderada de recursos de CPU adicionais.

Ativar Deduplicação: selecione esta opção para que cada bloco de entrada de dados seja comprimido e comparado com os 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 seleção da deduplicação é cancelada 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 bloco.

Criptografia Ativada: esta opção exibe o status de criptografia do host de armazenamento de backup primário ou secundário. A criptografia pode ser ativada somente durante a inicialização do vSnap. Essa opção não pode ser alterada nesta área de janela.



4. Clique em **Salvar**.

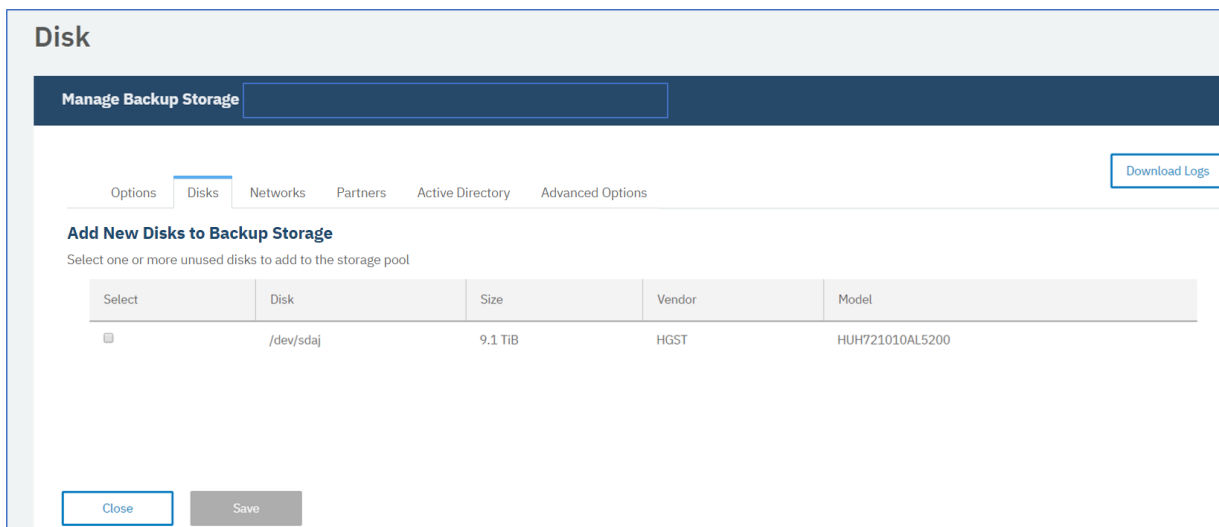
Incluindo novos discos no armazenamento de backup

Se você precisar de mais espaço para operações de backup em um conjunto de armazenamento selecionado, será possível incluir armazenamento em disco não utilizado. Isso se aplica aos armazenamentos de backup primário e secundário.

Procedimento

Para incluir novos discos não utilizados em um conjunto de armazenamento em disco, conclua as etapas a seguir:

1. Na navegação, clique em **Configuração do Sistema** , **Armazenamento de Backup** > **Disco**.
2. Na área de janela **Armazenamento em Disco**, clique no ícone gerenciar  que está associado ao servidor que você deseja editar.
3. Selecione um disco para incluir no seu ambiente de armazenamento a partir da lista de discos disponíveis na tabela **Incluir Novos Discos no Armazenamento de Backup**.



Select	Disk	Size	Vendor	Model
<input type="checkbox"/>	/dev/sdaj	9.1 TiB	HGST	HUH721010AL5200

4. Clique em **Salvar**.


Configurando controladores de interface de rede

É possível configurar seu armazenamento de backup primário e secundário para usar vários controladores de interface de rede (NICs) para diferentes funções específicas. Os NICs em seu ambiente do IBM Spectrum Protect Plus podem ser configurados para transferir dados para operações de backup, restauração e replicação. É possível configurar um NIC para transferências de dados de backup, restauração e replicação ou para transferências de dados de backup e restauração ou de replicação. Ao configurar NICs separados, é possível dedicar uma rede a operações de replicação e outra rede a operações de backup e restauração.

Antes de Iniciar

As versões do servidor vSnap anteriores à V10.1.6 não suportam esse recurso. Para atualizar um servidor vSnap, siga as instruções em [“Atualizando servidores vSnap”](#) na página 176.


Sobre Esta Tarefa

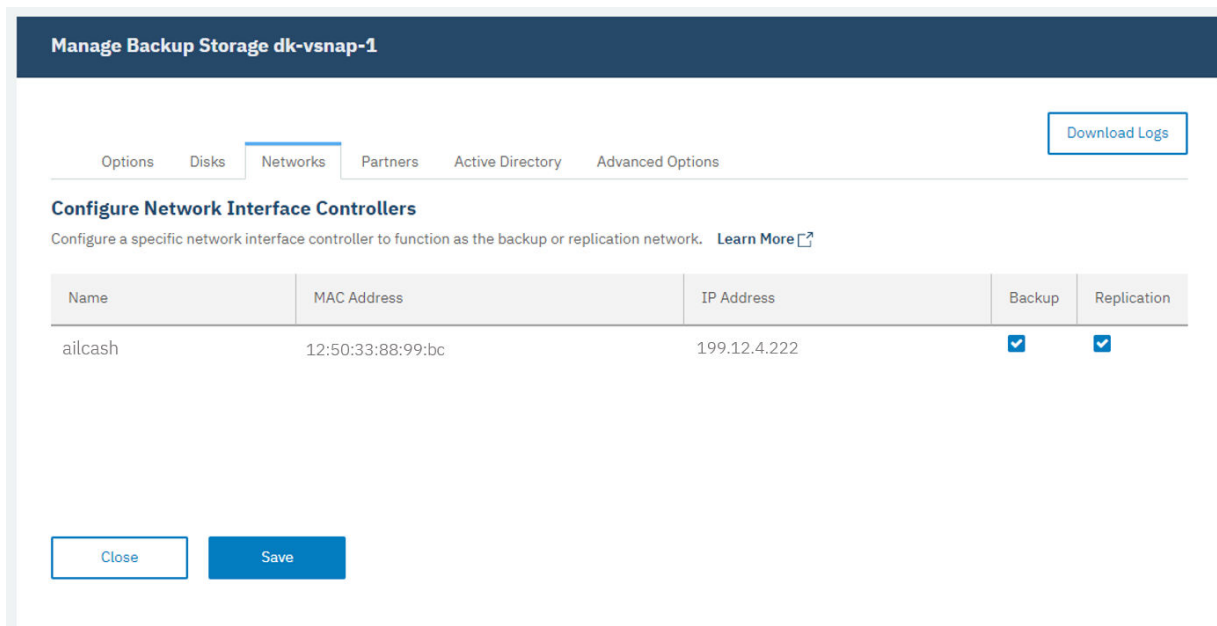
A rede que se dedica a enviar comandos de gerenciamento do IBM Spectrum Protect Plus para o servidor vSnap é indicada pelo ícone a seguir na página **Rede**, .

As conexões podem ser estabelecidas entre o servidor vSnap e uma gama de clientes, incluindo servidores de aplicativos, hosts de hypervisor, proxies VADP e qualquer outro componente em seu ambiente que transfira dados para e do armazenamento de backup.

Procedimento

Para configurar um NIC para operações de backup e replicação, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Configuração do sistema** , **Armazenamento de backup** > **Disco**.
2. Na guia **Redes**, selecione a configuração que você deseja para seus NICs listados:
 - Para configurar um NIC somente para transferências de dados para operações de backup e restauração, selecione **Backup**. Durante as operações de backup e restauração, as conexões são estabelecidas para o servidor vSnap usando o endereço IP desse NIC. Se a opção **Backup** for especificada por vários NICs, o primeiro que se conectar com sucesso será usado.
 - Para configurar um NIC para transferências de dados apenas para fins de replicação, selecione **Replicação**. Durante as operações de replicação de entrada para um servidor vSnap, as conexões são estabelecidas usando o endereço IP desse NIC no servidor vSnap de destino. Se a opção **Replicação** for especificada para vários NICs no servidor vSnap de destino, o primeiro endereço IP de destino que se conectar com sucesso a partir do servidor vSnap de origem será usado.
 - Para configurar um NIC para as transferências de dados de replicação, e de backup e restauração, selecione **Backup e Replicação**.



Manage Backup Storage dk-vsnap-1

Options Disks **Networks** Partners Active Directory Advanced Options [Download Logs](#)

Configure Network Interface Controllers
Configure a specific network interface controller to function as the backup or replication network. [Learn More](#)

Name	MAC Address	IP Address	Backup	Replication
ailcash	12:50:33:88:99:bc	199.12.4.222	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Close](#) [Save](#)

3. Clique em **Salvar**.

Configurando parceiros de armazenamento de backup


É possível configurar seus sites primários e secundários de armazenamento de backup para estabelecer parcerias de replicação com outros sites para estender seu ambiente. Depois de configurar parceiros de replicação, é possível copiar dados de um site para outro para uma camada adicional de proteção de dados.

Antes de Iniciar

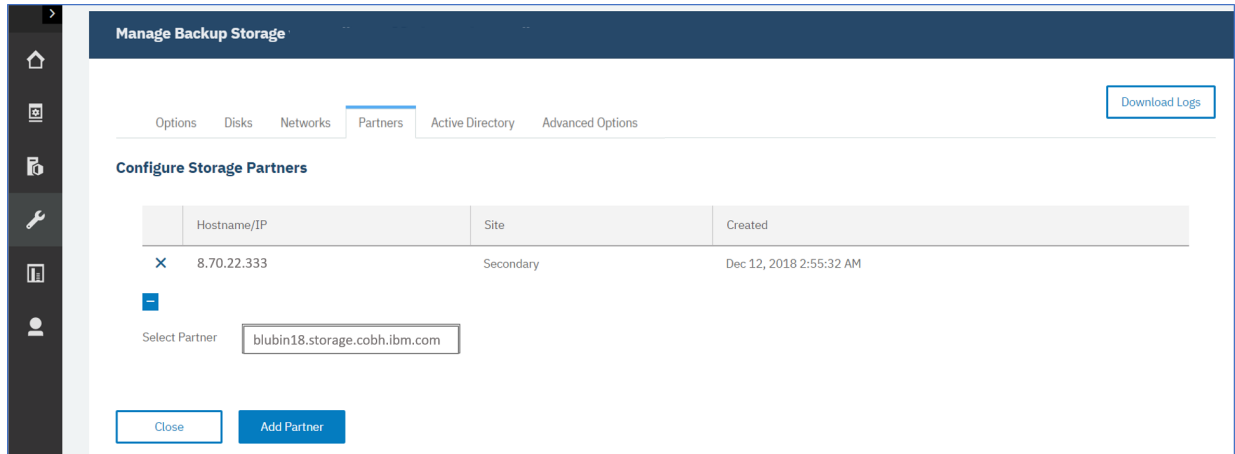
Todos os servidores vSnap devem estar no mesmo nível de versão para que a replicação funcione. A replicação entre diferentes versões não é suportada.

Procedimento

Para incluir parceiros em um servidor do seu ambiente de armazenamento, conclua as etapas a seguir:

1. Na navegação, clique em **Configuração do Sistema** , **Armazenamento de Backup** > **Disco**.
Os parceiros configurados que já foram incluídos são listados na tabela.

2. Na área de janela **Parceiros**, selecione um parceiro para incluir no host de armazenamento de backup primário ou secundário no menu suspenso.



3. Clique em **Incluir Parceiro** para incluir o parceiro e fechar a janela.

Configurando um Active Directory

Você pode associar seu armazenamento de backup primário e secundário a um domínio de diretório ativo. Quando o host primário ou secundário é adicionado a um domínio, quaisquer tarefas de backup de log do Microsoft SQL Server que estão associadas a esse host usam a autenticação de domínio para montar o volume de backup do log. Dessa forma, é possível evitar o requisito de usar uma área temporária local no servidor de aplicativos para operações de backup de log.

Antes de Iniciar

Você pode ter que configurar o servidor Domain Name System (DNS) para que o controlador de domínio esteja disponível para a rede e possa ser associado ao host primário ou secundário.

Procedimento

Para incluir um Active Directory para operações de backup e restauração, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Configuração do sistema**, **Armazenamento de backup** > **Disco**.
2. Na guia **Active Directory**, clique no ícone gerenciar que está associado ao host primário ou secundário que você deseja editar.
3. Insira o nome de domínio do Active Directory, juntamente com o nome de usuário e a senha para o administrador do Active Directory, conforme mostrado na figura a seguir.



4. Clique em **Associar**.

Configurando opções avançadas de armazenamento

É possível configurar opções avançadas relacionadas ao armazenamento para o armazenamento de backup primário ou secundário em seu ambiente.

Procedimento

Para configurar opções avançadas para seu armazenamento de backup, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Configuração do sistema** , **Armazenamento de backup** > **Disco**.
2. Na área de janela **Gerenciar Armazenamento de Backup**, clique no ícone de configurações  que está associado ao host que você está gerenciando.
3. Na guia **Opções Avançadas**, configure as opções avançadas conforme mostrado no exemplo a seguir:

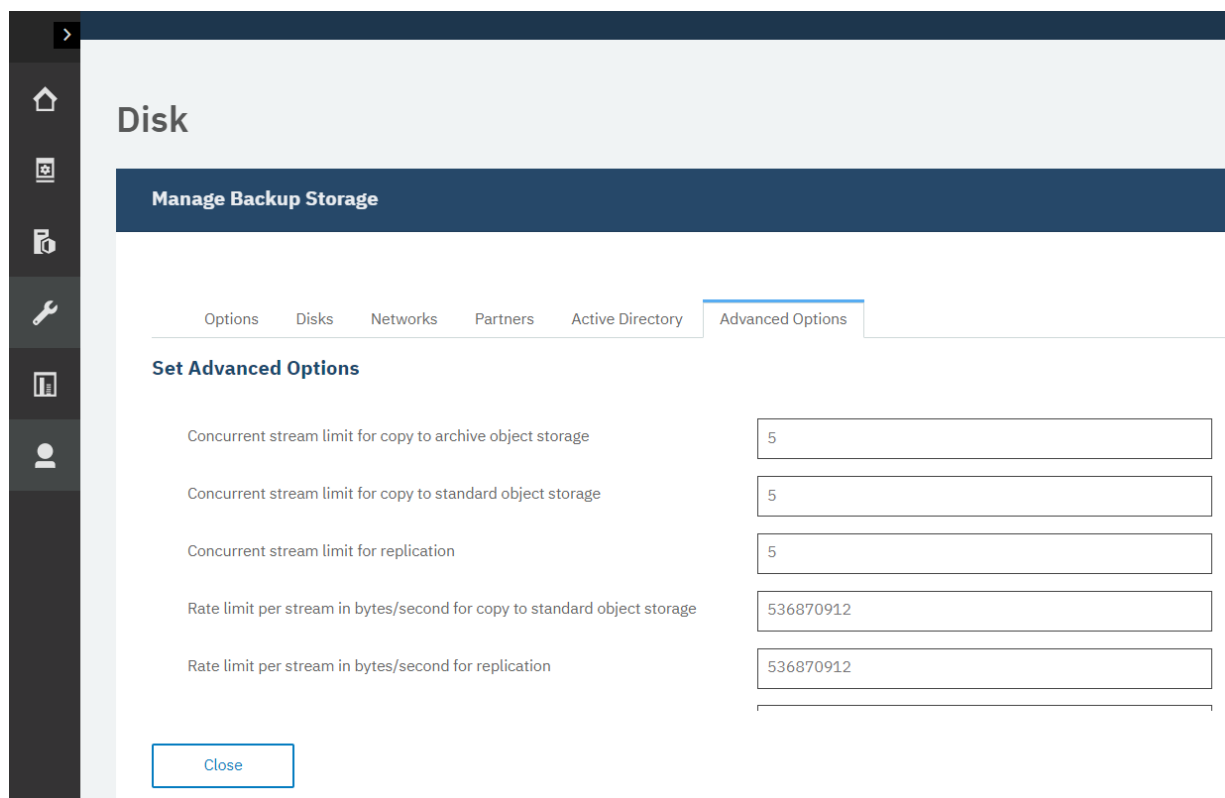


Figura 10. Gerenciar opções avançadas de armazenamento de backup.

- **Limite de fluxo simultâneo para cópia para armazenamento de objeto de archive:** esse valor define o número máximo de fluxos simultâneos que são usados por este host de backup quando você está copiando dados no Object Storage de archive.
- **Limite de fluxo simultâneo para cópia para armazenamento de objeto padrão:** esse valor define o número máximo de fluxos simultâneos que são usados por este host de backup quando você está copiando dados no Object Storage padrão.
- **Limite de fluxo simultâneo para replicação:** esse valor define o número máximo de fluxos simultâneos que são usados por este host de backup quando você está replicando dados para outros hosts de backup.
- **Limite de taxa por fluxo em bytes/segundo para cópia para armazenamento de objetos padrão:** esse valor define a taxa de transferência máxima em bytes por segundo que o host de backup usa para cada fluxo de dados quando você está copiando dados para o Object Armazenamento padrão. O valor especificado é o máximo na ausência de quaisquer outros fatores limitantes. A taxa real de cada fluxo de dados pode ser menor que este valor e depende de recursos do sistema disponíveis, de condições de rede e de qualquer limitação da largura de banda definida em opções do site.
- **Limite de taxa por fluxo em bytes/segundo para replicação:** esse valor define a taxa de transferência máxima em bytes por segundo que o host de backup usa para cada fluxo de dados quando você está replicando. O valor especificado é o máximo na ausência de quaisquer outros fatores limitantes. A taxa real de cada fluxo de dados pode ser menor que este valor e depende de recursos do sistema disponíveis, de condições de rede e de qualquer limitação da largura de banda definida em opções do site.
- **Camada de recuperação para restauração do armazenamento de objeto de archive do AWS (Bulk, Standard ou Expedited):** esse valor especifica a camada de recuperação que é usada por este host de backup durante operações de restauração do Object Storage de archive do Amazon Glacier. Esse valor deve ser especificado como Bulk, Standard ou Expedited. A camada de recuperação pode ser modificada para atingir tempos de operação de restauração mais rápidos no custo de encargos de dados mais elevados. Para obter informações sobre as opções de camada de

recuperação disponíveis e a precificação associada, consulte a documentação do Amazon Web Services.


- **Backup Simultâneo:** esta opção especifica o número máximo de fluxos de backup paralelos para o host quando várias tarefas são executadas simultaneamente. Para operações de backup de aplicativo, cada banco de dados é tratado como um fluxo único. Para operações de backup do hypervisor, cada disco virtual é tratado como um fluxo único. As opções de backup simultâneas podem ser usadas para evitar que políticas de SLA múltiplas ou grandes enviem fluxos de dados em excesso para um pequeno host de backup que não possa acomodar a carga. Para reduzir o tempo de processamento para operações de backup, configure esta opção para uma das opções a seguir:

Ilimitado: um número ilimitado de fluxos de backup simultâneos pode ser executado.

Pausa: para pausar o uso deste host de backup. As tarefas que tentarem utilizar esse host de backup serão pausadas enquanto essa configuração estiver selecionada. Essa opção deve ser usada em situações em que o host de backup requer manutenção emergencial e que o impedirá temporariamente de ser usado por quaisquer tarefas.

Limite: para definir um limite máximo sobre o número de fluxos de backup que podem ser executados simultaneamente. Insira um valor numérico especificando o número máximo de fluxos simultâneos.

Dica: Quando você altera um valor de opção, o novo valor é aplicado quando você clica no campo de

opção seguinte. Ao lado da opção atualizada, a mensagem a seguir é exibida,  **Updated**.

4. Clique em **Concluir**.

Como excluir e recriar um conjunto de armazenamentos do vSnap?


Quando surge um cenário que resulta no requisito de excluir um conjunto de armazenamento vSnap devido à distorção ou a qualquer outro motivo, é possível seguir as etapas para excluir e recriar o conjunto de armazenamento. Este procedimento é uma operação destrutiva que descarta todos os dados em um conjunto de armazenamento vSnap existente. Todos os dados de backup no conjunto são perdidos e não são mais recuperáveis, portanto, é necessário cuidado antes de continuar. Depois que isso for feito, você pode criar um conjunto vazio de substituição.

Procedimento

1. Para se preparar para a remoção de um conjunto de armazenamento, deve-se primeiro cancelar o registro do servidor vSnap removendo-o.

Para obter mais informações sobre como cancelar o registro do servidor vSnap, consulte [“Cancelando o registro de um servidor vSnap”](#) na página 116.

2. Execute uma tarefa de manutenção no servidor vSnap abrindo **Tarefa e Operações > Planejamento**.

Encontre a tarefa *Manutenção* na lista. Clique no ícone de ações,  e clique em **Iniciar**.

Quando a tarefa de manutenção é concluída, todas as informações sobre o servidor vSnap são removidas do catálogo do SPP. Todos os pontos de recuperação e metadados que estão associados aos backups da VM, e todas as cópias de réplica que são armazenados no vSnap não registrado, são removidos. Todos os dados são removidos e não estão mais disponíveis para recuperação.

Para obter mais informações sobre tarefas de manutenção, consulte [“Tipos de Tarefa”](#) na página 495.

3. No servidor vSnap, execute o comando a seguir para inicializar o servidor vSnap limpo.

```
$ vsnap system init --skip_pool
```

Se o sistema foi inicializado anteriormente, é seguro executar este comando novamente. Esta etapa garante que os módulos de kernel necessários sejam instalados e carregados.

4. Identifique o identificador do conjunto de armazenamentos existente executando o comando a seguir:

```
$ vsnap pool show
```

Se o conjunto de armazenamento estiver on-line, o identificador será exibido no campo *ID*. Se o conjunto de armazenamento estiver off-line, será exibida uma mensagem de erro que indica que as informações do conjunto não podem ser exibidas. O identificador do conjunto é mostrado nesta mensagem de erro.

5. Execute o comando delete para o identificador do conjunto de armazenamentos para excluir forçosamente o conjunto de armazenamento.

```
$ vsnap pool delete --id <ID> --force
```

Quando o comando for concluído, a mensagem a seguir será exibida:

```
0 conjunto de armazenamento foi excluído com sucesso, mas o conjunto não foi desmontado
porque a opção 'force' foi configurada.
Reinicialize o sistema para assegurar que os discos que foram usados anteriormente sejam
liberados.
```

6. Reinicie o sistema para liberar quaisquer discos que ainda estejam em uso. Insira o seguinte comando:

```
$ sudo reboot -n
```

É importante reiniciar o sistema depois de executar este comando para assegurar que quaisquer discos que ainda estão em uso por conjuntos mais antigos sejam liberados.

7. Quando a reinicialização for finalizada, execute o comando status:

```
$ vsnap_status
```

A saída desse comando mostra o status de todos os serviços do servidor vSnap. Assegure-se de que todos os serviços estejam ativos. Se um ou mais serviços estiverem ativando, verifique o status posteriormente até que estejam todos no estado ativo.

8. Identifique os discos que devem ser incluídos no conjunto.

Se você estiver reutilizando o mesmo conjunto de discos que compõe o conjunto antigo, o comando a seguir poderá ajudá-lo a identificá-los:

```
$ vsnap disk show
```

Na saída do comando show, a coluna **USED AS** indica se um sistema de arquivos ou uma tabela de partição existe no disco. Os discos que faziam parte do conjunto antigo são identificados como vsnap_pool. Se o conjunto antigo foi criptografado, alguns ou todos os discos podem ser identificados como crypto_LUKS.

Saída de Amostra

UUID	TYPE	VENDOR	MODEL	SIZE	USED AS
KNAME NAME					

6000c299371bdc647c80720602079bc	SCSI	VMware	Virtual disk	70.00GB	LVM2_member
sda /dev/sda					
6000c29b8ea25349e3a884d58f72e640	SCSI	VMware	Virtual disk	100.00GB	vsnap_pool
sdb /dev/sdb					
6000c297cb8078cf9f56ab688a326a24	SCSI	VMware	Virtual disk	128.00GB	LVM2_member
sdc /dev/sdc					
6000c2950248c5d831b6661ab0ec8843	SCSI	VMware	Virtual disk	16.00GB	vsnap_pool
sdd /dev/sdd					
6000c29359661cbd915a7f24c8b44cf8	SCSI	VMware	Virtual disk	16.00GB	vsnap_pool
sde /dev/sde					

9. **Importante:** O comando nessa etapa exclui tabelas de partição e metadados do sistema de arquivos dos discos especificados e os marca como não utilizados. Use esse comando com cuidado e assegure-se de especificar apenas discos que não estão mais em uso.

Execute o comando a seguir para especificar uma lista separada por vírgula de nomes de discos para marcar como não utilizados.

```
$ vsnap disk wipe <disk_list>
```

O comando a seguir é um exemplo do comando de limpeza do disco: `$ vsnap disk wipe /dev/sdb,/dev/sdd,/dev/sde`.

10. Crie o novo conjunto com o seguinte comando:

```
$ vsnap pool create --name <pool_name> <options> --disk_list <disk_list>
```

Em que *pool_name* é o nome do novo conjunto; *options* especifica o tipo de RAID ou opções de criptografia. Deixar essa opção em branco aplica as opções padrão. *disk_list* representa a lista separada por vírgula de discos a serem adicionados ao conjunto. Os discos que você especificar devem ter um status de unused na execução do comando **vsnap disk show**.

O comando a seguir é um exemplo do comando create:

```
$ vsnap pool create --name primary --disk_list /dev/sdb,/dev/sdd
```

Quando você estiver especificando a lista de discos, especifique apenas os discos que você pretende usar como os discos de dados principais. Os discos de cache ou de log podem ser adicionados posteriormente executando comandos separados. Para obter mais informações sobre recomendações e instruções para configurar os discos de cache e de log, consulte o [Blueprints](#).

Dica:

Para abrir a ajuda, execute o comando `vsnap pool create --help`.

11. Para visualizar as informações do conjunto, execute o comando a seguir:

```
$ vsnap pool show
```

Assegure-se de que o comando exiba as informações corretas do conjunto e de que o comando seja concluído sem um erro.

12. Registre o servidor vSnap no IBM Spectrum Protect Plus em um site escolhido para finalizar a configuração.

Para obter mais informações sobre como registrar um servidor vSnap, consulte [“Registrando um servidor vSnap como um provedor de armazenamento de backup”](#) na página 115.

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. Trata-se de um processo único que deve ser executado para novas instalações.

Sobre Esta Tarefa

Durante o processo de inicialização, o vSnap cria um conjunto de armazenamentos usando quaisquer discos não utilizados disponíveis conectados ao sistema para uma instalação física. Se nenhum disco não utilizado for localizado, o processo de inicialização será concluído sem criar um conjunto. Para uma implementação virtual do vSnap, um disco virtual não utilizado padrão de 100 GB é definido e usado para criar o conjunto.

Para obter informações sobre como expandir, criar e administrar conjuntos de armazenamentos, consulte [“Gerenciamento de armazenamento”](#) na página 131.

Você pode usar a interface com o usuário do IBM Spectrum Protect Plus ou a interface da linha de comando (CLI) do vSnap para inicializar servidores vSnap.

Para servidores que são implementados e incluídos em IBM Spectrum Protect Plus, a interface com o usuário do IBM Spectrum Protect Plus fornece um método simples para executar a operação de inicialização.

Para servidores que são implementados em um ambiente físico, a interface da linha de comandos (CLI) do 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 o vSnap integrado que é instalado como parte de uma instalação do IBM Spectrum Protect Plus, é solicitado que você inicie o processo de inicialização na primeira vez que efetuar login na interface com o usuário. Nenhuma etapa adicional é necessária. O servidor vSnap que está no site Demo incluído com o IBM Spectrum Protect Plus deve ser usado apenas para propósitos de teste e demo e nunca como um destino de backup em um ambiente de produção.

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. A partir do ícone de menu de 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 é implementado em seu ambiente. 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` usando SSH. Quando implantado virtualmente, a senha inicial é `sppDP758 -SysXyz`. Será solicitado que você altere essa senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#). Se implementado fisicamente, use a senha que você criou para a conta `serveradmin` durante a instalação.

Você também pode usar um ID do usuário que tenha privilégios de vSnap que foi criado anteriormente 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 129](#).

2. Emita o comando **\$ vsnap system init** com a opção **--skip_pool** para inicializar o servidor do vSnap sem criar um conjunto de armazenamento. A conclusão do processo pode levar de 5 a 10 minutos. Emita o seguinte comando:

```
$ vsnap system init --skip_pool
```

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 131 .

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.

Antes de Iniciar

Os discos virtuais ou físicos devem ser adicionados ao servidor vSnap antes deste procedimento. A expansão dos volumes existentes não é suportada.

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.

Mudando a taxa de rendimento

Altere o rendimento para replicação do site e operações de cópia para que você possa gerenciar sua 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.

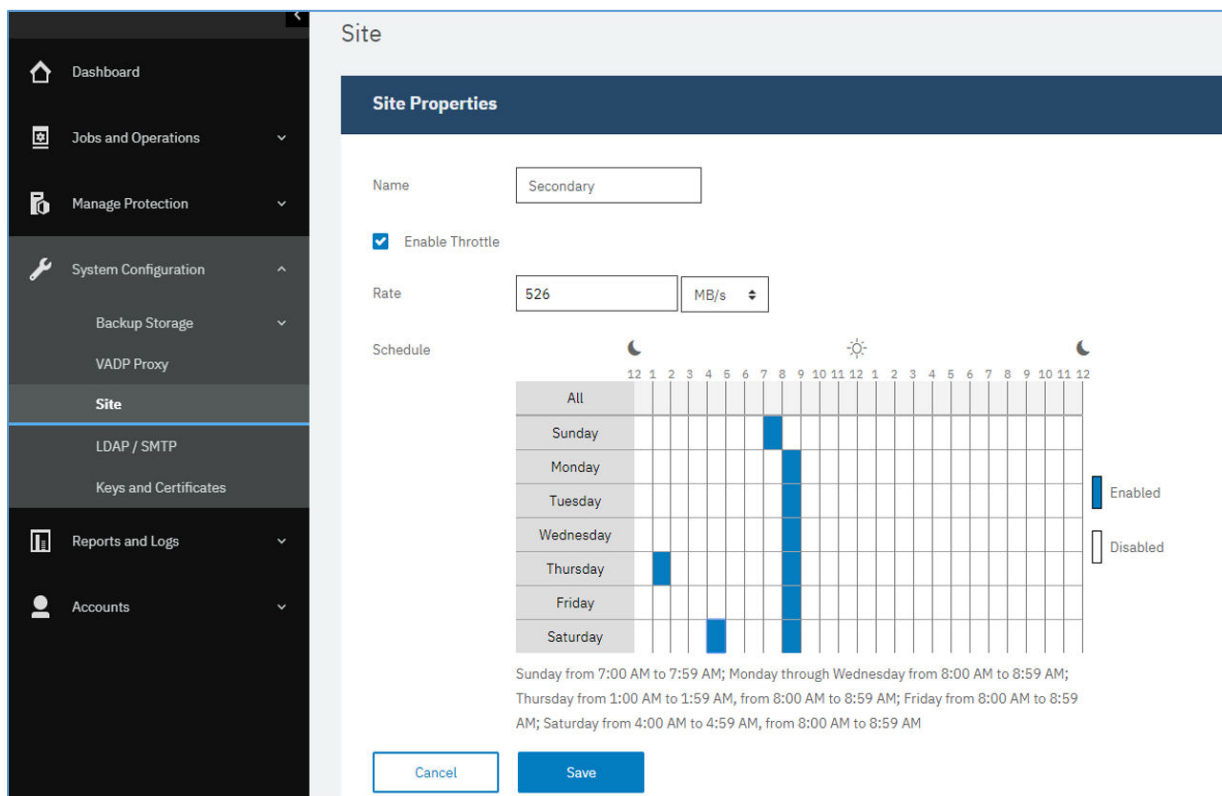


Figura 11. Ativando diferentes reguladores para diferentes horários para melhorar o rendimento

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.

Substituindo um servidor vSnap com falha

Em um ambiente IBM Spectrum Protect Plus, o servidor vSnap de destino é o destino para backup de dados. Se o servidor vSnap for corrompido ou falhar ao responder, será possível substituí-lo por um novo servidor e recuperar os dados armazenados.

Antes de Iniciar

Importante: Não cancele o registro do servidor vSnap com falha do IBM Spectrum Protect Plus. O servidor com falha deve permanecer registrado para que o procedimento de substituição funcione corretamente.

Um ou mais servidores de réplica do vSnap inicializados devem existir no ambiente para que esse processo seja concluído com sucesso.

Sobre Esta Tarefa

O procedimento para substituir um servidor vSnap com falha é documentado na [nota técnica 1103847](#).

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.


Você pode ter que configurar e administrar determinados aspectos do vSnap, como configuração de rede ou gerenciamento do conjunto de armazenamento.

Gerenciando o vSnap usando a interface da linha de comandos

O servidor vSnap pode ser gerenciado por meio da interface da linha de comandos e é o principal meio de administração de um servidor vSnap. Execute o comando **vsnap** a partir da interface do servidor vSnap após a conexão por meio do SSH usando o ID do usuário `serveradmin` ou qualquer outro usuário do sistema operacional ao qual tenham sido designados privilégios de administrador vSnap. A senha inicial do `serveradmin` é `sppDP758 -SysXyz`. É solicitado que mude esta senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).

A interface da linha de comandos consiste em vários comandos e sub-comandos que gerenciam vários aspectos do sistema. Você também pode passar a sinalização **-- help** para qualquer comando ou subcomando para visualizar 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  de um servidor vSnap para editar suas configurações.

Tarefas relacionadas

[“Gerenciando servidores vSnap” na página 115](#)

Para ativar tarefas de backup e restauração, o IBM Spectrum Protect Plus requer pelo menos um servidor vSnap. O servidor vSnap é seu próprio dispositivo, implementado virtualmente ou instalado fisicamente em um sistema que atenda aos requisitos mínimos. Cada servidor vSnap no ambiente deve ser registrado no IBM Spectrum Protect Plus para ser reconhecido. O servidor vSnap que está registrado no site Demo que é incluído com o IBM Spectrum Protect Plus deve ser usado apenas para propósitos de teste e demonstração, e nunca deve ser utilizado como um destino de backup em um ambiente de produção.

[“Configurando opções avançadas de armazenamento” na página 122](#)

É possível configurar opções avançadas relacionadas ao armazenamento para o armazenamento de backup primário ou secundário em seu ambiente.

Gerenciamento do Usuário

É possível gerenciar usuários do servidor vSnap emitindo o comando **vsnap user**. Esse comando e as opções disponíveis são usados para criar usuários, conceder e revogar privilégios do usuário, consultar usuários e atualizar a senha de um usuário.

Os usuários que são criados em um servidor vSnap são usuários do sistema operacional que são incluídos no grupo de sistema operacional vSnap. Usuários no grupo de sistema operacional vSnap não recebem privilégios **sudo**. Como resultado, esses usuários requerem uma senha para executar um comando.

É possível criar um usuário vSnap emitindo o comando **create**. Dessa forma, você cria um usuário do sistema operacional que é designado ao grupo **vsnap** que pode executar comandos vSnap e fazer chamadas da API. Emita o comando **create**:

```
$ vsnap user create
```

Se estiver funcionando interativamente, você será solicitado a inserir o nome do usuário, a senha e a senha uma segunda vez para confirmação. Se estiver executando de forma não interativa, as opções a seguir estarão disponíveis para o comando **create**:

--username <username>

Insira o nome do usuário.

--password <password>

Insira a senha do usuário.

É possível conceder privilégios a uma conta do sistema operacional existente para assegurar que o usuário possa executar comandos vSnap e fazer chamadas de API. Para conceder privilégios, emita o comando **grant**:

```
$ vsnap user grant
```

Se estiver funcionando interativamente, você será solicitado a inserir o nome do usuário, a senha e a senha uma segunda vez para confirmação. Se estiver executando de forma não interativa, as opções a seguir estarão disponíveis para o comando **grant**:

--username <username>

Insira o nome do usuário.

--password <password>

Insira a senha do usuário. Essa deve ser a senha da conta do sistema operacional se a conta já existir no sistema.

É possível revogar privilégios de um usuário que é designado ao grupo **vsnap**. O usuário permanecerá como um usuário do sistema operacional mas não será mais capaz de executar comandos vSnap ou fazer chamadas de API. Para revogar privilégios, emita o comando **revoke**:

```
$ vsnap user revoke
```

Se estiver executando de forma interativa, será solicitado que você insira o nome do usuário. Se estiver executando de forma não interativa, as opções a seguir estarão disponíveis para o comando **revoke**:

--username <username>

Insira o nome do usuário.

Para exibir uma lista de usuários do vSnap que fazem parte do grupo **vsnap** no servidor vSnap, emita o comando **show**:

```
$ vsnap user show
```

Um usuário do vSnap pode ter a senha da conta alterada, que atualizará a senha desse usuário no sistema. Emita o comando **update**:

```
$ vsnap user update
```

Se estiver executando de forma interativa, será solicitado que você insira o nome do usuário, a senha antiga, a nova senha e a nova senha uma segunda vez para confirmação. Se estiver executando de forma não interativa, as opções a seguir estarão disponíveis para o comando **update**:

--username <username>

Insira o nome do usuário.

--password <old_password>

Digite a senha antiga do usuário.

--new_password <new_password>

Digite a nova senha do usuário.

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 os 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 já podem

ter uma redundância externa ativada por meio de um controlador RAID de hardware, mas se não, 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.



Atenção: Uma vez que um disco foi adicionado a um conjunto de armazenamento, ele não deve ser removido. A remoção de um disco corromperá o conjunto de armazenamento.

Se o vSnap foi implementado como parte de um dispositivo virtual, ele já contém um disco virtual inicial de 100 GB. Revise os detalhes em [Blueprints](#) para obter informações sobre como manipular esse disco e como removê-lo. 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 utilizem configurações RAID e utilizem VMDKs thick provisioned. A replicação para servidores vSnap externos fornece proteção adicional.

Um servidor vSnap se tornará invalidado se o conjunto vSnap for excluído ou se um disco vSnap for excluído. 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 chaves de criptografia de disco gerados na criação do conjunto são armazenados sob o diretório `/etc/vsnap/keys/` em cada servidor vSnap. Para fins de recuperação de desastres, faça backup dos arquivos de chave manualmente para outro local fora do servidor vSnap. Depois que um conjunto for criado, use os seguintes comandos como o usuário `serveradmin` para copiar as chaves para um local temporário e, em seguida, copiá-las para um local de backup desejado e seguro fora do host vSnap.

Primeiro, crie um diretório no qual as chaves serão submetidas a backup.

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

Em seguida, copie os arquivos-chave para o local temporário.


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

Por fim, copie o diretório `keybackup-<hostname>`, em que *<hostname>* é o nome atribuído ao servidor vSnap para um local de backup seguro fora do host vSnap.

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 ícone de menu de ações  ao lado do 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 armazenamento.

Criando um conjunto de armazenamentos

Se você concluiu o procedimento de inicialização simples descrito em [“Concluindo uma inicialização simples”](#) na página 127, 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 133. Para obter informações sobre opções disponíveis, passe a opção **-- 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 133](#).

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  de um servidor vSnap para gerenciá-lo, e, em seguida, expanda a guia **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.

A rede em um servidor vSnap pode ser modificada através da interface da linha de comandos (CLI) por meio do uso do comando **network**. Informações adicionais podem ser obtidas usando a opção `-- help` após qualquer comando.

Mostrando informações da interface de rede

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

```
$ vsnap network show
```

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

mgmt

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

repl

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

nfs

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

smb

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

iscsi

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

Modificando Serviços Associados às Interfaces de Rede

Execute o comando **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.

```
$ vsnap network update
```

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. Os seguintes são valores válidos: **mgmt**, **repl**, **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.

Instalando cabeçalhos e ferramentas do kernel

Cabeçalhos e ferramentas do kernel não são instalados por padrão. Se você planeja compilar e usar drivers customizados, módulos ou outros softwares, instale o cabeçalho ou ferramenta do kernel apropriado no servidor vSnap.

Sobre Esta Tarefa

Quando o vSnap é instalado ou atualizado, o Linux kernel Versão 4.19 é instalado por padrão. Se você optar por não fazer o upgrade do kernel para a V4.19 e permanecer no V3.10, um kernel V3.10 compatível com o servidor vSnap será instalado e usado. Em ambos os casos, cabeçalhos e ferramentas de kernel associados ao kernel não serão instalados. Se pretende compilar ou usar drivers customizados, módulos ou outro software, você deve instalar os pacotes do kernel. Os instaladores do Red Hat Package Manager (RPM) para os cabeçalhos e ferramentas do kernel estão disponíveis no diretório de instalação do vSnap.

Procedimento

1. Efetue login no servidor vSnap como o usuário **serveradmin**. A senha inicial é **sppDP758-SysXyz**. É solicitado que mude esta senha durante o primeiro login. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).
2. Para determinar a versão do kernel do Linux, abra uma linha de comandos e emita o comando a seguir:

```
$ uname -r
```

A saída é exibida, em que **xxxx** representa o número de revisão do kernel:

```
$ 4.19.xxxx
```

3. Navegue para este diretório:

```
$ cd /opt/vsnap/config/pkgs/kernel/
```

4. No diretório, localize o arquivo **xxxxxxxx.rpm**, que é o pacote a ser instalado. Certifique-se de que o pacote correto seja identificado para a versão do kernel do Linux instalada. Para instalar o cabeçalho ou ferramenta do kernel, emita o comando a seguir:

```
$ sudo yum localinstall xxxxxxxx.rpm
```

Resultados

O cabeçalho ou ferramenta do kernel está instalado.

Resolução de problemas de servidores vSnap

Os servidores vSnap em um ambiente do IBM Spectrum Protect Plus fornecem armazenamento em disco para proteção de dados por meio de processos de backup e de replicação. O servidor vSnap configurado em seu ambiente pode ser usado como o destino, a origem ou o servidor e o destino. Para reparar ou substituir um servidor vSnap que falhou, há etapas a serem seguidas para que o servidor vSnap afetado seja trazido para um estado de trabalho primeiro para que os serviços de backup e replicação possam ser retomados. Isso é para assegurar a perda mínima de dados.

Evitando falhas de tarefa sincronizando as senhas do vSnap e CIFS

As comunicações entre um servidor vSnap e um compartilhamento do Common Internet File System (CIFS) podem ser interrompidas se as credenciais forem compartilhadas, mas as senhas estiverem fora de sincronização. Para evitar que as tarefas falhem, você deve sincronizar as senhas do vSnap e CIFS.

Sobre Esta Tarefa

Para obter informações sobre como sincronizar senhas, consulte [“Gerenciamento do Usuário” na página 130](#).

Por que o servidor vSnap ainda está off-line?

Depois que você reiniciar o servidor vSnap, ele continuará mostrando um status de off-line na interface com o usuário do IBM Spectrum Protect Plus.

Se a deduplicação de dados estiver ativada ou foi ativada anteriormente em um servidor vSnap, a tabela de deduplicação (DDT) será pré-carregada na memória durante o processo de inicialização do servidor vSnap. O processo de pré-carregamento da DDT pode introduzir um atraso de 15 minutos na inicialização dos serviços do servidor vSnap. Durante esse tempo, o vSnap server mostra com um status de *Offline* é exibido. Aguarde pelo menos 15 minutos para que o processo seja concluído e para que o servidor vSnap retorne para o status *Online*. É possível executar o comando `vsnap_status` para monitorar os serviços do servidor vSnap.

Se algum dos serviços do vSnap estiver no estado *activating*, isso significa que os serviços do vSnap estão iniciando. Quando todos os serviços estiverem no estado *active*, o servidor vSnap está on-line novamente.

Posso reparar um servidor vSnap com falha no ambiente do IBM Spectrum Protect Plus?

Os servidores vSnap que estão configurados em seu ambiente IBM Spectrum Protect Plus fornecem armazenamento em disco para proteção de seus dados por meio de processos de backup e replicação. Se um dos servidores vSnap em seu ambiente falhar ou precisar ser substituído, é necessário executar etapas para reparar e depois restaurar os dados que estão armazenados lá e para que ele possa fornecer serviços de backup e replicação com sucesso.

Sobre Esta Tarefa

Importante:

Nota: supõe-se que todos os servidores vSnap no ambiente sejam protegidos pela replicação. Se um servidor vSnap não for replicado e for perdido, ele não poderá ser recuperado para um estado para continuar atuando em sua função como armazenamento em disco de origem ou de destino. Na ausência

de replicação, deve-se criar novos servidores vSnap e configurar políticas de acordo de nível de serviço (SLA). Quando isso é executado, um novo processo de backup completo ocorre.

Um servidor vSnap pode funcionar em seu ambiente nas funções a seguir:

- vSnap como o armazenamento em disco de *origem* para operações de backup
- vSnap como o armazenamento em disco de *destino* para operações de replicação a partir de outro servidor vSnap
- Servidor vSnap que serve tanto de *origem* quanto de *destino* para serviços de backup e replicação.

A operação de reparo foi projetada para recuperar um servidor vSnap para um estado para permitir que ele continue o processamento normal. Os resultados da operação de reparo dependem das funções do servidor vSnap que está sendo reparado:

- Se você estiver reparando um servidor vSnap de origem, a operação de reparo recuperará o ponto de recuperação mais recente do servidor vSnap de destino para que as operações de backup possam continuar processando mudanças incrementais das cargas de trabalho de produção e não necessitará de um backup completo. Observe, nesse caso, que os pontos de recuperação anteriores ao ponto de recuperação mais recente no servidor vSnap de origem não serão restaurados, mas ainda estarão disponíveis para recuperação e reutilização no servidor vSnap de destino.
- Se você estiver reparando um servidor vSnap de destino, a operação de reparo restabelecerá o relacionamento para que a próxima operação de replicação possa ser executada normalmente. O processo de reparo não transferirá nenhum dado. Após a conclusão do processo de reparo, o processamento continuará da seguinte forma:
 - Os dados de backup incremental serão enviados para o servidor vSnap de origem e de destino por execução de planejamento de SLA.
 - A tarefa de replicação iniciará por planejamento de SLA e replicará todos os pontos de recuperação criados no servidor vSnap de origem após a execução do processo de reparo. Neste momento, os dados serão replicados do servidor vSnap de origem para o servidor vSnap de destino. Trata-se de uma transferência de dados completa de todos os dados necessários para representar os pontos de recuperação mais recentes, conforme mencionado acima.

Dependendo da função do servidor vSnap, siga as orientações nas seções abaixo:

Procedimento

Como reparar um vSnap de origem com falha em um ambiente do IBM Spectrum Protect Plus?

Os servidores vSnap em um ambiente do IBM Spectrum Protect Plus fornecem armazenamento em disco para proteção de dados por meio de processos de backup e de replicação. É possível reparar e substituir um servidor vSnap com falha que está configurado em seu ambiente IBM Spectrum Protect Plus para agir como a *origem* para serviços de backup e replicação. O servidor vSnap de origem deve ser reparado para que os serviços de backup e de replicação possam continuar.

Antes de Iniciar

Importante: Supõe-se que todos os servidores vSnap no ambiente sejam protegidos por replicação. Se um servidor vSnap não for replicado e ele falhar, ele não poderá ser recuperado para um estado que permitiria que ele continuasse como uma origem ou um destino de armazenamento em disco. Na ausência de processos de replicação, deve-se criar um novo servidor vSnap e configurar políticas de acordo de nível de serviço (SLA). Quando você executa as políticas, um novo processo de backup completo é executado para o novo servidor vSnap.

Para determinar qual tipo de processo de reparo é aplicável ao seu servidor vSnap, consulte a [nota técnica 1103847](#).

Sobre Esta Tarefa

Importante: Não cancele o registro ou exclua o servidor vSnap com falha por meio do IBM Spectrum Protect Plus. O servidor vSnap com falha deve permanecer registrado para que o procedimento de substituição funcione corretamente.

Este procedimento estabelece um novo servidor vSnap de origem em seu ambiente IBM Spectrum Protect Plus para substituir o servidor vSnap de origem com falha. O novo servidor vSnap de origem conterá apenas os pontos de recuperação mais recentes.

Nota: A versão do novo servidor vSnap deve corresponder à versão do dispositivo IBM Spectrum Protect Plus implementado.

Procedimento

1. Efetue login no console do servidor vSnap de destino com o ID serveradmin usando o protocolo Secure Shell (SSH).

Insira o comando a seguir: `$ ssh serveradmin@MGMT_ADDRESS`

Por exemplo, `$ ssh serveradmin@10.10.10.2`

2. Obtenha o ID do servidor vSnap de origem com falha abrindo um prompt de comando e inserindo o seguinte comando:

`$ vsnap partner show`

A saída é semelhante ao seguinte exemplo:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
PORTA da API: 8900
Porta de SSH: 22
```

3. Verifique se o MGMT ADDRESS é o endereço do servidor vSnap de origem com falha. Anote o número do ID do servidor vSnap de origem com falha.
4. No ambiente com o servidor vSnap de origem, instale um novo servidor vSnap do mesmo tipo e versão, e mesma alocação de armazenamento, que o servidor vSnap de origem com falha.

Para obter instruções sobre a instalação de um servidor vSnap, consulte [Instalando um servidor vSnap físico](#).

Importante: Não registre o novo servidor vSnap com o IBM Spectrum Protect Plus. Não use o assistente Incluir armazenamento em disco.

- a) Você primeiro precisará inicializar o servidor vSnap com o comando a seguir:

`$ vsnap system init ----skip_pool id partner_id`

Por exemplo: `$ vsnap system init --skip_pool --id 12345678901234567890123456789012` usando o ID do parceiro do vSnap de origem com falha. Uma mensagem indica quando a inicialização é concluída.

Nota: Este comando é diferente para o comando de inicialização do vSnap listado no IBM Knowledge Center e nos Blueprints.

5. Complete o processo de criação do servidor vSnap e do conjunto como esboçado em *Capítulo 5: Instalação e configuração do servidor vSnap* nos [Blueprints](#).
6. Coloque o novo servidor vSnap de origem no modo de manutenção, inserindo o seguinte comando:

`$ vsnap system maintenance begin`

Colocar o servidor vSnap em modo de manutenção suspende operações, como criação de captura instantânea, tarefas de restauração de dados e operações de replicação.

7. Inicialize o novo servidor vSnap de origem com o ID do parceiro do servidor vSnap de origem com falha. Insira o seguinte comando:

`$ vsnap system init --id partner_id`

O comando a seguir é um exemplo: `$ vsnap system init --id 12345678901234567890123456789012`

8. No novo servidor vSnap de origem, inclua os servidores vSnap parceiros. Cada parceiro deve ser incluído separadamente. Para incluir um parceiro, insira o comando a seguir:

```
$ vsnap partner add --remote_addr remote_ip_address --local_addr local_ip_address
```

em que, *remote_ip_address* especifica o endereço IP do servidor vSnap de origem e *local_ip_address* especifica o endereço IP do novo servidor vSnap de origem.

O comando a seguir é um exemplo:

```
$ vsnap partner add --remote_addr 10.10.10.2 --local_addr 10.10.10.1
```

9. Quando solicitado, digite o ID do usuário e a senha para o servidor vSnap de destino.
As mensagens informativas indicam quando os parceiros são criados e atualizados com sucesso.
10. Crie uma tarefa de reparo no novo servidor vSnap de origem, inserindo o comando a seguir:

```
$ vsnap repair create --async
```

A saída desse comando é semelhante ao exemplo a seguir:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: Não
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDENTE
MESSAGE: 0 reparo foi planejado
```

11. Monitore o número de volumes que estão envolvidos na operação de reparo inserindo o comando a seguir:

```
$ vsnap repair show
```

A saída desse comando é semelhante ao exemplo a seguir:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: Não
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ATIVO
MESSAGE: Created 0 volumes. There are 3 primary volumes that have recoverable snapshots,
the latest snapshot of each will be restored. Restoring 3 snapshots: 3 active, 0 pending, 0
completed, and 0 failed
```

O número de volumes que estão envolvidos na operação de reparo é indicado no campo VOLUMES TOTAIS.

12. Monitore o status da tarefa de reparo visualizando o arquivo `repair.log` no novo servidor vSnap de origem, no diretório a seguir `/opt/vsnap/log/repair.log`. Como alternativa, é possível inserir o comando a seguir:

```
$ vsnap repair show
```

A saída desse comando é semelhante ao exemplo anterior. As mensagens de status a seguir podem ser exibidas durante o processo de reparo:

- STATUS: PENDING indica que a tarefa de reparo está prestes a ser executada.
- STATUS: ACTIVE indica que a tarefa de reparo está ativa.

- STATUS: COMPLETED indica que a tarefa de reparo está concluída.
 - STATUS: FAILED indica que a tarefa de reparo falhou e deve ser reenviada.
13. Durante a operação de reparo, execute o comando mostrar reparo do vSnap para verificar quando o status está CONCLUÍDO.

```
$ vsnap repair session show
```

A saída desse comando é semelhante ao exemplo a seguir:

```
ID: 1 RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ATIVO
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
Created 0 volumes.
There are 3 replica volumes whose snapshots will be restored on next replication.
```

É exibida uma sessão para cada volume envolvido na operação de reparo.

Periodicamente, emita o comando `$ vsnap repair session show` para assegurar que a quantidade de dados que estão sendo enviados para cada volume esteja aumentando em incrementos. À medida que as sessões terminam, você verá a mudança de status para COMPLETED. Quando todas as sessões terminarem, emita o comando `$ vsnap repair session show` para verificar se o status geral é COMPLETED. É exibida uma mensagem final indicando o número de volumes para os quais foram restaurados capturas instantâneas. A saída de mensagem é semelhante ao exemplo a seguir:

```
Created 0 volumes.
There are 3 primary volumes that have recoverable snapshots, the latest snapshot of each
will be restored.
Restored 3 snapshots.
```

14. Para quaisquer capturas instantâneas que não forem restauradas e que indiquem um status FAILED, reenvie o processo de reparo, inserindo o seguinte comando:

```
$ vsnap repair create --async --retry
```

15. Quando o processo de reparo relatar um status COMPLETED, será possível continuar as operações normais para o servidor vSna, movendo-o para fora do modo de manutenção. Para continuar o processamento normal, insira o comando a seguir:

```
$ vsnap system maintenance complete
```

16. Remova as chaves do host de SSH salvas do servidor de vSnap de origem reparado e dos servidores vSnap de destino.

Execute os comandos a seguir nos servidores vSnap de origem e de destino:

```
$ sudo rm -f /home/vsnap/.ssh/known_hosts
```

```
$ sudo rm -f /root/.ssh/known_hosts
```

A remoção das chaves SSH assegura que as transferências de replicação subsequentes não produzam erros que resultem da chave de host mudada do servidor vSnap reparado.

17. Reinicie o serviço do vSnap no servidor substituído inserindo o comando a seguir:

```
$ sudo systemctl restart vsnap
```

18. Clique em **Configuração do sistema > Armazenamento de backup > Disco** para verificar se o novo servidor vSnap está registrado corretamente, conforme a seguir:

- Se o novo servidor vSnap estiver usando o mesmo nome do host ou endereço IP para registro, nenhuma mudança será necessária.

- Se o novo servidor vSnap estiver usando um nome de host ou endereço IP diferente para registro, você deverá atualizar o registro, selecionando o ícone do lápis.
19. Para remover pontos de recuperação que não estiverem mais disponíveis no servidor vSnap de origem, inicie uma tarefa de manutenção por meio da interface com o usuário do IBM Spectrum Protect Plus.

Para obter instruções, consulte [Criando tarefas e planejamentos de tarefa](#).

Dica: Você pode ver mensagens informativas que são semelhantes ao exemplo a seguir:

```
Captura instantânea de armazenamento spp_1004_2102_2_16de41fcbc3 do CTGGA1843 não localizada no vsnap em tempo real de Tipo de captura instantânea Storage2101
```

20. Para continuar as tarefas que falharam depois que o servidor vSnap ficou indisponível, execute uma tarefa de inventário do servidor de armazenamento. Para obter instruções, consulte [Criando tarefas e planejamentos de tarefa](#).

Resultados

O servidor vSnap de origem foi reparado com apenas os pontos de recuperação mais recentes. A próxima tarefa de backup executada como parte de um SLA fará backup de dados incrementalmente. Se você criar uma tarefa de restauração, apenas o ponto de recuperação mais recente estará disponível no repositório de backup. Todos os outros pontos de recuperação estarão disponíveis nos repositórios de replicação e nos repositórios de armazenamento de objeto e archive, se aplicável ao seu ambiente.

Como reparar um vSnap de destino com falha em um ambiente IBM Spectrum Protect Plus?

Os servidores vSnap em um ambiente do IBM Spectrum Protect Plus fornecem armazenamento em disco para proteção de dados por meio de processos de backup e de replicação. É possível reparar e substituir um servidor vSnap com falha que está configurado em seu ambiente IBM Spectrum Protect Plus para agir como o *destino* para serviços de backup e replicação. O servidor vSnap de origem deve ser reparado para que os serviços de backup e de replicação possam continuar.

Antes de Iniciar

Importante: Supõe-se que todos os servidores vSnap no ambiente sejam protegidos por replicação. Se um servidor vSnap não for replicado e ele falhar, ele não poderá ser recuperado para um estado que permitiria que ele continuasse como uma origem ou um destino de armazenamento em disco. Na ausência de processos de replicação, deve-se criar um novo servidor vSnap e configurar políticas de acordo de nível de serviço (SLA). Quando você executa as políticas, um novo processo de backup completo é executado para o novo servidor vSnap.

Sobre Esta Tarefa

Importante: Não cancele o registro ou exclua o servidor vSnap com falha por meio do IBM Spectrum Protect Plus. O servidor vSnap com falha deve permanecer registrado para que o procedimento de substituição funcione corretamente.

Esse procedimento estabelece um novo servidor vSnap de destino em seu ambiente IBM Spectrum Protect Plus para substituir o servidor vSnap de destino com falha. O novo servidor vSnap de destino não conterá nenhum dado, mas será preenchido com os pontos de recuperação mais recentes durante a próxima operação de replicação planejada.

Nota: A versão do novo servidor vSnap deve corresponder à versão do dispositivo IBM Spectrum Protect Plus implementado.

Para determinar qual tipo de processo de reparo é aplicável ao seu servidor vSnap, consulte a [nota técnica 1103847](#).

Procedimento

1. Efetue login no console do servidor vSnap em funcionamento com o ID serveradmin usando o protocolo Secure Shell (SSH).

Insira o comando a seguir: `$ ssh serveradmin@MGMT_ADDRESS`

Por exemplo, `$ ssh serveradmin@10.10.10.1`

2. Obtenha o ID do servidor vSnap com falha abrindo um prompt de comandos e inserindo o comando a seguir:

```
$ vsnap partner show
```

A saída é semelhante ao seguinte exemplo:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.2
PORTA da API: 8900
Porta de SSH: 22
```

3. Verifique se o MGMT ADDRESS é o endereço do servidor vSnap com falha. Anote o número de ID do servidor vSnap com falha.
4. No ambiente com o servidor vSnap de destino, instale um novo servidor vSnap do mesmo tipo e versão, e com a mesma alocação de armazenamento, conforme o servidor vSnap de destino com falha.

Para obter instruções sobre a instalação de um servidor vSnap, consulte [Instalando um servidor vSnap físico](#).

Importante: Não registre o novo servidor vSnap com o IBM Spectrum Protect Plus. Não use o assistente Incluir armazenamento em disco.

- a) Você primeiro precisará inicializar o servidor vSnap com o comando a seguir:

```
$ vsnap system init --skip_pool --id <partner_id>
```

Por exemplo: `$ vsnap system init --skip_pool --id 12345678901234567890123456789012` usando o ID do parceiro do vSnap de origem com falha. Uma mensagem indica quando a inicialização é concluída.

Nota: Este comando é diferente para o comando de inicialização do vSnap listado no IBM Knowledge Center e nos Blueprints.

5. Complete o processo de criação do servidor vSnap e do conjunto como esboçado em *Capítulo 5: Instalação e configuração do servidor vSnap* nos [Blueprints](#).
6. Coloque o novo servidor vSnap no modo de manutenção, inserindo o comando a seguir:

```
$ vsnap system maintenance begin
```

Colocar o servidor vSnap em modo de manutenção suspende operações, como criação de captura instantânea, tarefas de restauração de dados e operações de replicação.

7. Inicialize o novo servidor vSnap de destino com o ID do parceiro do servidor vSnap de destino com falha. Insira o seguinte comando:

```
$ vsnap system init --id <partner_id>
```

O comando a seguir é um exemplo:

```
$ vsnap system init --id 12345678901234567890123456789012
```

8. No novo servidor vSnap de destino, inclua os servidores vSnap do parceiro. Cada parceiro deve ser incluído separadamente. Para incluir um parceiro, insira o comando a seguir:

```
$ vsnap partner add --remote_addr <remote_ip_address> --local_addr <local_ip_address>
```

em que, `<remote_ip_address>` especifica o endereço IP do servidor vSnap de origem e `<local_ip_address>` especifica o endereço IP do novo servidor vSnap de destino.

O comando a seguir é um exemplo:

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

9. Quando solicitado, insira o ID do usuário e a senha para o servidor vSnap de origem.

As mensagens informativas indicam quando os parceiros são criados e atualizados com sucesso.

10. Crie uma tarefa de reparo no novo servidor vSnap de origem, inserindo o comando a seguir:

```
$ vsnap repair create --async
```

A saída desse comando é semelhante ao exemplo a seguir:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: Não
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDENTE
MESSAGE: The repair has been scheduled
```

11. Monitore o número de volumes que estão envolvidos na operação de reparo inserindo o comando a seguir:

```
$ vsnap repair show
```

A saída desse comando é semelhante ao exemplo a seguir:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: Não
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ATIVO
MESSAGE: Creating 3 volumes for partner 670d61a10f78456bb895b87c45e20999
```

O número de volumes que estão envolvidos na operação de reparo é indicado no campo TOTAL VOLUMES.

12. Monitore o status da tarefa de reparo visualizando o arquivo `repair.log` no novo servidor vSnap de origem, no diretório a seguir `/opt/vsnap/log/repair.log`. Como alternativa, é possível inserir o comando a seguir:

```
$ vsnap repair show
```

A saída desse comando é semelhante ao exemplo anterior. As mensagens de status a seguir podem ser exibidas durante o processo de reparo:

- STATUS: PENDING indica que a tarefa de reparo está prestes a ser executada.
- STATUS: ACTIVE indica que a tarefa de reparo está ativa.
- STATUS: COMPLETED indica que a tarefa de reparo está concluída.
- STATUS: FAILED indica que a tarefa de reparo falhou e deve ser reenviada.

13. Durante a operação de reparo, execute o comando `mostrar reparo` do vSnap para verificar quando o status está CONCLUÍDO.

```
$ vsnap repair session show
```

A mensagem final indica o número de volumes cujas capturas instantâneas serão restauradas na próxima replicação, conforme a seguir:

```
Criados 0 volumes.  
Há três volumes de réplica cujas capturas instantâneas serão restauradas na próxima replicação.
```

14. Para quaisquer capturas instantâneas que não forem restauradas e indicarem um status FAILED, reenvie o processo de reparo, inserindo o comando a seguir:

```
$ vsnap repair create --async --retry
```

15. Quando o processo de reparo relatar um status COMPLETED, será possível continuar as operações normais para o servidor vSna, movendo-o para fora do modo de manutenção. Para continuar o processamento normal, insira o comando a seguir:

```
$ vsnap system maintenance complete
```

16. Remova as chaves do host de SSH salvas do servidor de vSnap de origem reparado e dos servidores vSnap de destino.

Execute os comandos a seguir nos servidores vSnap de origem e de destino:

```
$ sudo rm -f /home/vsnap/.ssh/<known_hosts>
```

```
$ sudo rm -f /root/.ssh/<known_hosts>
```

A remoção das chaves SSH assegura que as transferências de replicação subsequentes não produzam erros que resultem da chave de host mudada do servidor vSnap reparado.

17. Reinicie o serviço vSnap no servidor substituído inserindo o comando a seguir.

```
$ sudo systemctl restart vsnap
```

18. Clique em **Configuração do Sistema > Armazenamento de Backup > Disco** para verificar se o novo vSnap está registrado corretamente da seguinte forma:

- Se o novo servidor vSnap estiver usando o mesmo nome do host ou endereço IP para registro, nenhuma mudança será necessária.
- Se o novo servidor vSnap estiver usando um nome do host ou um endereço IP diferente para registro, você deverá atualizar o registro selecionando o ícone de lápis.

19. Para remover pontos de recuperação que não estiverem mais disponíveis no servidor vSnap de origem, inicie uma tarefa de manutenção por meio da interface com o usuário do IBM Spectrum Protect Plus.

Dica: Você pode ver mensagens informativas que são semelhantes ao exemplo a seguir:

```
Captura instantânea de armazenamento spp_1004_2102_2_16de41fcbc3 do CTGGA1843 não localizada no vsnap em tempo real de Tipo de captura instantânea Storage2101
```

20. Para continuar as tarefas que falharam depois que o servidor vSnap ficou indisponível, execute uma tarefa de inventário do servidor de armazenamento.

Resultados

O servidor vSnap de destino foi reparado. Uma nova tarefa de backup deve ser executada no servidor vSnap de origem antes de qualquer ação adicional ser tomada no novo servidor vSnap de destino.

Se uma tarefa de replicação for tentada no novo servidor vSnap de destino, uma mensagem será exibida da seguinte forma:

```
CTGGA0289 - Skipping volume <volume_id> because there are no new snapshots since last backup
```

Depois que uma nova tarefa de backup é executada no servidor vSnap de origem, a próxima tarefa de replicação planejada replica os pontos de recuperação criados pela tarefa de backup. Nesse ponto, se

you create a restore task, only the most recent recovery point will be available in the replication repository. If the vSnap destination server was also acting as the source of the copy for the storage of objects or archives, the replication task must be executed first on the vSnap destination server before any additional copy operation can be completed successfully. The first copy of data for the storage of objects will be a full copy.

Como reparar um vSnap de dupla função com falha em um ambiente do IBM Spectrum Protect Plus?

It is possible to repair and replace a vSnap server that is configured in the environment of your IBM Spectrum Protect Plus to act as the *origem* and the *destino* for backup and replication services.

Sobre Esta Tarefa

Importante: Não cancele o registro ou exclua o servidor vSnap com falha do IBM Spectrum Protect Plus. O servidor vSnap com falha deve permanecer registrado para que o procedimento de substituição funcione corretamente.

This procedure establishes a new vSnap server in your IBM Spectrum Protect Plus environment to replace the vSnap server with the failure. After the repair process is complete, the new vSnap server is recovered to a point in time where backup tasks can continue to make backup of incremental changes (without the need for a full backup) and replication tasks can continue.

To determine what type of repair process is applicable to your vSnap server, consult the [technical note 1103847](#).

Nota: A versão do novo servidor vSnap deve corresponder à versão do dispositivo IBM Spectrum Protect Plus implementado.

Procedimento

1. Log in to the vSnap server in operation in your environment console with the ID `serveradmin` using the Secure Shell (SSH) protocol.
Enter the command as follows: `$ ssh serveradmin@MGMT_ADDRESS`
For example, `$ ssh serveradmin@10.10.10.2`
2. Obtain the ID of the vSnap server with the failure by opening a command prompt and entering the command as follows:

```
$ vsnap partner show
```

The output is similar to the following example:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
PORTA da API: 8900
Porta de SSH: 22
```

3. Verify that the MGMT ADDRESS is the address of the vSnap server with the failure. Note the ID number of the vSnap server with the failure.
4. On the vSnap destination server, install a new vSnap server of the same type and version, and with the same storage allocation, as the vSnap server with the failure.
For instructions on installing a vSnap server, consult [Installing a physical vSnap server](#).

Importante: Não registre o novo servidor vSnap com o IBM Spectrum Protect Plus. Não use o assistente Incluir armazenamento em disco.

- a) You must first initialize the vSnap server with the command as follows:

```
$ vsnap system init ----skip_pool id partner_id
```

Por exemplo: `$ vsnap system init --skip_pool --id 12345678901234567890123456789012` usando o ID do parceiro do vSnap de origem com falha. Uma mensagem indica quando a inicialização é concluída.

Nota: Este comando é diferente para o comando de inicialização do vSnap listado no IBM Knowledge Center e nos Blueprints.

5. Complete o processo de criação do servidor vSnap e do conjunto como esboçado em *Capítulo 5: Instalação e configuração do servidor vSnap* nos [Blueprints](#).

6. Coloque o novo servidor vSnap no modo de manutenção, inserindo o comando a seguir:

```
$ vsnap system maintenance begin
```

Colocar o servidor vSnap em modo de manutenção suspende operações, como criação de captura instantânea, tarefas de restauração de dados e operações de replicação.

7. Inicialize o novo servidor vSnap de destino com o ID do parceiro do servidor vSnap de destino com falha. Insira o comando a seguir para inicializar o vSnap:

```
$ vsnap system init --id partner_id
```

O comando a seguir é um exemplo: `$ vsnap system init --id 12345678901234567890123456789012`

8. No novo servidor vSnap de destino, inclua os servidores vSnap do parceiro. Se houver mais de um servidor parceiro, cada parceiro deve ser incluído separadamente. Para incluir um parceiro, insira o comando a seguir:

```
$ vsnap partner add --remote_addr remote_ip_address --local_addr local_ip_address
```

em que, `remote_ip_address` especifica o endereço IP do servidor vSnap de origem e `local_ip_address` especifica o endereço IP do novo servidor vSnap de destino.

O comando a seguir é um exemplo:

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

9. Quando solicitado, insira o ID do usuário e a senha para o servidor vSnap de origem.

As mensagens informativas indicam quando os parceiros são criados e atualizados com sucesso.

10. Crie uma tarefa de reparo no novo servidor vSnap de origem, inserindo o comando a seguir:

```
$ vsnap repair create --async
```

A saída desse comando é semelhante ao exemplo a seguir:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: Não
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDENTE
MESSAGE: 0 reparo foi planejado
```

11. Monitore o número de volumes que estão envolvidos na operação de reparo inserindo o comando a seguir:

```
$ vsnap repair show
```

A saída desse comando é semelhante ao exemplo a seguir:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 6
SNAPSHOTS RESTORED: N/A
RETRY: Não
CREATED: 2019-11-01 15:49:31 UTC
```



```
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ATIVO
MESSAGE: Created 0 volumes
There are 3 replica volumes whose snapshots will be restored on next replication.
There are 3 primary volumes that have recoverable snapshots, the latest snapshot of each
will be restored.
The number of volumes that are involved in the repair operation are indicated in the TOTAL
VOLUMES field
```

12. Monitore o status da tarefa de reparo visualizando o arquivo `repair.log` no novo servidor vSnap de origem, no diretório a seguir `/opt/vsnap/log/repair.log`. Como alternativa, é possível inserir o comando a seguir:

```
$ vsnap repair show
```

13. Quando o status da operação de reparo estiver no estado `ACTIVE`, é possível visualizar o status das sessões de reparo individuais, inserindo o seguinte comando:

```
$ vsnap repair session show
```

A saída é semelhante a este exemplo:

```
ID: 1
RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ATIVO
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
```

Visualize uma sessão para cada um dos volumes de origem na operação de reparo. A quantidade de dados que são enviados para cada volume mostra valores incrementais crescentes até que o processo seja concluído. A mensagem final indica o número de volumes cujas capturas instantâneas serão restauradas pela próxima operação de replicação, conforme mostrado neste exemplo:

```
Criados 0 volumes. Há três volumes de réplica cujas capturas instantâneas serão restauradas
na próxima replicação.
```

14. Para quaisquer capturas instantâneas que não forem restauradas e indicarem um status `FAILED`, reenvie o processo de reparo, inserindo o comando a seguir:

```
$ vsnap repair create --async --retry
```

15. Quando o processo de reparo relatar um status `COMPLETED`, será possível continuar as operações normais para o servidor vSna, movendo-o para fora do modo de manutenção. Para continuar o processamento normal, insira o comando a seguir:

```
$ vsnap system maintenance complete
```

16. Opcional: Para visualizar o total de volumes e o número de capturas instantâneas que foram restaurados durante a operação de reparo, execute o comando `show` para o servidor vSnap.

A saída inclui as seguintes informações:

- **Total** volumes lista o número total de volumes que foram inspecionados durante a operação de reparo. Essa lista inclui os volumes de origem (volumes primários) em que o backup do ponto de recuperação mais recente foi restaurado e os volumes de destino (volumes de réplica) que são preenchidos novamente durante as próximas operações de replicação, conforme planejado em SLAs.
- **SNAPSHOTS RESTORED** lista o número de volumes de origem que foram restaurados.

17. Remova as chaves do host de SSH salvas do servidor de vSnap de origem reparado e dos servidores vSnap de destino.

Execute os comandos a seguir nos servidores vSnap de origem e de destino:

```
$ sudo rm -f /home/vsnap/.ssh/known_hosts
```

```
$ sudo rm -f /root/.ssh/known_hosts
```

A remoção das chaves SSH assegura que as transferências de replicação subsequentes não produzam erros que resultem da chave de host mudada do servidor vSnap reparado.

18. Reinicie o serviço do vSnap no servidor substituído inserindo o comando a seguir:

```
$ sudo systemctl restart vsnap
```

19. Clique em **Configuração do sistema > Armazenamento de backup > Disco** para verificar se o novo servidor vSnap está registrado corretamente, conforme a seguir:

- Se o novo servidor vSnap estiver usando o mesmo nome do host ou endereço IP para registro, nenhuma mudança será necessária.
- Se o novo servidor vSnap estiver usando um nome do host ou um endereço IP diferente para registro, você deverá atualizar o registro selecionando o ícone de lápis.

20. Para remover pontos de recuperação que não estão mais disponíveis no servidor vSnap de origem, inicie uma tarefa de manutenção a partir da interface com o usuário do IBM Spectrum Protect Plus. Siga as instruções aqui para fazer isso, [Criando tarefas e planejamentos de tarefas](#).

Dica: Você pode ver mensagens informativas que são semelhantes ao exemplo a seguir:

```
CTGGA1843 storage snapshot spp_1005_2102_2_16de41fcbc3 not found on live Storage2101  
Snapshot Type vsnap
```

21. Para continuar as tarefas que falharam depois que o servidor vSnap ficou indisponível, execute uma tarefa de inventário do servidor de armazenamento. Para obter instruções, consulte [Criando tarefas e planejamentos de tarefa](#).

Resultados

Para os dados de backup primários que são armazenados no servidor vSnap reparado, o ponto de recuperação mais recente para os dados de backup primário agora está disponível. Os backups subsequentes para o servidor vSnap reparado continuam a enviar apenas mudanças incrementais desde o último backup. Para os dados replicados armazenados no servidor de vSnap reparado, nenhum dado replicado fica imediatamente disponível após o reparo. As tarefas de replicação subsequentes do servidor parceiro vSnap preencherão novamente quaisquer backups que forem criados no servidor parceiro vSnap após a conclusão do processo de reparo. Se uma tarefa de replicação for tentada no servidor parceiro vSnap antes de um backup ser concluído no servidor parceiro vSnap, será exibida uma mensagem de aviso indicando que não há novas capturas instantâneas desde o último backup:

```
CTGGA0289 - Skipping volume <volume_id> because there are no new snapshots since last backup
```

Se o servidor vSnap reparado estivesse atuando como uma fonte de cópia para o armazenamento de objeto ou archive, uma tarefa de backup deve ser primeiro executada no servidor vSnap reparado antes de qualquer operação de cópia adicional seja bem-sucedida. A primeira cópia de dados para o armazenamento de objetos será uma cópia completa.

Capítulo 5. Instalando o Suporte de Backup de Kubernetes

Para proteger volumes persistentes em contêineres, o administrador de backup deve instalar e configurar Suporte de Backup de Kubernetes no ambiente de Kubernetes.

Pré-requisitos para o Suporte de Backup de Kubernetes

Antes de instalar o Suporte de Backup de Kubernetes, assegure-se de que todos os requisitos do sistema e pré-requisitos sejam atendidos.

Para requisitos do sistema Suporte de Backup de Kubernetes, consulte [“Requisitos do Suporte de Backup de Kubernetes”](#) na página 54.

Em seguida, para atender aos pré-requisitos para Suporte de Backup de Kubernetes, complete as seguintes ações no ambiente de Kubernetes:

- [“Ativando o recurso VolumeSnapshotDataSource”](#) na página 149
- [“Verificando se o Metrics Server está em execução”](#) na página 150
- [“Definindo o relacionamento entre o aplicativo e a solicitação de volume persistente”](#) na página 151
- [“Criando um segredo de extração de imagem para usar com um registro externo”](#) na página 151

Ativando o recurso VolumeSnapshotDataSource

Para Kubernetes 1.16 apenas: é necessário ativar o recurso alfa **VolumeSnapshotDataSource** para suportar operações de backup de cópia e restauração de captura instantânea.

Para obter mais informações sobre os recursos alfa, consulte [Feature Gates](#).

Para ativar o recurso alfa **VolumeSnapshotDataSource**, você deve corrigir o planejador de Kubernetes, o controlador e o servidor da API da seguinte forma:

1. Usando o comando **sudo**, edite os arquivos YAML a seguir:

```
/etc/kubernetes/manifests/kube-apiserver.yaml  
/etc/kubernetes/manifests/kube-controller-manager.yaml  
/etc/kubernetes/manifests/kube-scheduler.yaml
```

2. Em cada arquivo YAML, inclua a instrução a seguir dentro da seção de comando:

```
--feature-gates=VolumeSnapshotDataSource=true
```

Importante: Assegure-se de editar os arquivos YAML diretamente e não crie cópias de backup desses arquivos no mesmo diretório. A presença das cópias de backup no diretório `/etc/kubernetes/manifests` pode anular as alterações que você fez para ativar a porta de recursos **VolumeSnapshotDataSource**.

Talvez seja necessário esperar um ou dois minutos para que as mudanças sejam detectadas pelo Kubernetes.

3. Verifique se o recurso está ativado emitindo os comandos a seguir:

```
ps aux | grep apiserver | grep feature-gates
```

```
ps aux | grep scheduler | grep feature-gates
```

```
ps aux | grep controller-manager | grep feature-gates
```

A saída para um desses comandos é semelhante ao exemplo a seguir:

```

root      13121  7.4  2.5 518276 305424 ?          Ssl  Sep06 120:37 kube-apiserver --
authorization-mode=Node,RBAC --advertise-address=192.0.2.0
--allow-privileged=true --client-ca-file=/etc/kubernetes/pki/ca.crt --enable-admission-
plugins=NodeRestriction --enable-bootstrap-token-auth=true
--etcd-cafile=/etc/kubernetes/pki/etcd/ca.crt --etcd-certfile=/etc/kubernetes/pki/apiserver-
etcd-client.crt --etcd-keyfile=/etc/kubernetes/pki/apiserver-etcd-client.key
--etcd-servers=https://127.0.0.1:2379 --insecure-port=0 --kubectl-client-certificate=/etc/
kubernetes/pki/apiserver-kubectl-client.crt
--kubectl-client-key=/etc/kubernetes/pki/apiserver-kubectl-client.key --kubectl-preferred-
address-types=InternalIP,ExternalIP,Hostname
--proxy-client-cert-file=/etc/kubernetes/pki/front-proxy-client.crt --proxy-client-key-
file=/etc/kubernetes/pki/front-proxy-client.key
--requestheader-allowed-names=front-proxy-client --requestheader-client-ca-file=/etc/
kubernetes/pki/front-proxy-ca.crt
--requestheader-extra-headers-prefix=X-Remote-Extra- --requestheader-group-headers=X-Remote-
Group --requestheader-username-headers=X-Remote-User
--secure-port=6443 --service-account-key-file=/etc/kubernetes/pki/sa.pub --service-cluster-
ip-range=198.51.100.0/24 --tls-cert-file=/etc/kubernetes/pki/apiserver.crt
--tls-private-key-file=/etc/kubernetes/pki/apiserver.key --feature-
gates=VolumeSnapshotDataSource=true

```

Verificando se o Metrics Server está em execução

Opcional: para ajudar a otimizar o desempenho e a escalabilidade do produto, assegure-se de que o Kubernetes Metrics Server v0.3.5 ou posterior esteja instalado e em execução adequadamente em seu cluster. O Metrics Server é usado pelo planejador Suporte de Backup de Kubernetes para determinar os recursos que são usados pelas instâncias do movedor de dados simultâneas.

Se o Metrics Server não retornar dados, o número de movedores de dados que são usados para operações de backup é limitado, o que pode impactar negativamente o desempenho.

Para obter instruções sobre como implementar o Metrics Server, revise o arquivo README.md em <https://github.com/kubernetes-sigs/metrics-server>. Para obter informações sobre o Kubernetes Metrics Server, consulte [Pipeline de métricas de recursos](#).

É possível verificar se o Metrics Server está instalado e retornando dados de métricas concluindo as etapas a seguir:

1. Verifique a instalação emitindo o seguinte comando:

```
kubectl get deploy,svc -n kube-system | egrep metrics-server
```

A saída é semelhante ao seguinte exemplo:

```

deployment.extensions/metrics-server 1/1 1 1 3d4h
service/metrics-server ClusterIP 198.51.100.0 <none> 443/TCP 3d4h

```

2. Verifique se o Metrics Server está retornando dados para todos os nós emitindo o comando a seguir:

```
kubectl get --raw "/apis/metrics.k8s.io/v1beta1/nodes"
```

A saída é semelhante ao seguinte exemplo:

```

{"kind": "NodeMetricsList", "apiVersion": "metrics.k8s.io/v1beta1", "metadata": {"selfLink": "/
apis/metrics.k8s.io/v1beta1/nodes"}, "items": [{"metadata":
{"name": "cirrus12", "selfLink": "/apis/metrics.k8s.io/v1beta1/nodes/cirrus12",
"creationTimestamp": "2019-08-08T23:59:49Z", "timestamp": "2019-08-08T23:59:08Z",
"window": "30s", "usage": {"cpu": "1738876098n", "memory": "8406880Ki"}}}]

```

Dica: O comando pode falhar com a saída vazia para a chave "items". Provavelmente esse erro é causado pela instalação do Metrics Server com um certificado autoassinado. Para resolver esse problema, instale o Metrics Server com um certificado assinado corretamente que seja reconhecido pelo cluster.

Definindo o relacionamento entre o aplicativo e a solicitação de volume persistente

Opcionalmente, você pode conectar seus aplicativos stateful a suas solicitações de volume persistente (PVCs) usando um relacionamento dependente de proprietário. Ao definir esse relacionamento, você ativa ações em cascata para os aplicativos.

Por exemplo, ajustar a escala de um aplicativo para cima ou para baixo pode fazer com que os backups planejados de seu PVC sejam pausados e retomados. Da mesma forma, a exclusão do aplicativo causa a exclusão da PVC, que, por sua vez, aciona a exclusão dos backups.

Depois que um aplicativo começa a usar uma PVC para armazenar dados persistentes, é possível reconfigurar a definição da PVC com seu aplicativo proprietário.

O exemplo a seguir é um arquivo de configuração de amostra para uma PVC que mostra o relacionamento dependente de proprietário entre um aplicativo e um objeto PVC. O objeto PVC inclui os detalhes da implementação do proprietário.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadados:
  name: demo-pvc
  ownerReferences:
    - apiVersion: apps/v1beta1
      blockOwnerDeletion: true
      kind: Deployment
      name: Dept10-deployment
      uid: 3b760e89-7da5-11e9-8c5a-0050568ba59c
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    pedidos:
      storage: 1Gi
  storageClassName: csi-rbd
```

Criando um segredo de extração de imagem para usar com um registro externo

Se você planeja extrair uma imagem de um registro ou repositório externo do Docker, deve-se criar um segredo de extração de imagem. Durante a implantação, o Kubernetes extrai os contêineres necessários do registro externo e fornece os pods para Suporte de Backup de Kubernetes.

O segredo de extração de imagem é usado para fornecer as credenciais que são necessárias pelo Kubernetes para extrair imagens do docker do registro externo.

O nome do segredo de extração de imagem que você cria deve corresponder ao valor para o parâmetro `PRODUCT_IMAGE_REGISTRY_SECRET_NAME` no arquivo de configuração `baas_config.cfg`.

O segredo de extração de imagem deve estar em todos os espaços de nomes das PVCs que serão protegidas por Suporte de Backup de Kubernetes.

Este procedimento não é necessário se você estiver usando um registro do Docker interno. Para um registro interno, especifique uma sequência vazia ("") para o parâmetro `PRODUCT_IMAGE_REGISTRY_SECRET_NAME`.

Dica: Se você estiver instalando Suporte de Backup de Kubernetes a partir do IBM Helm Chart Repository e IBM Entitled Registry, consulte o arquivo README do produto em <https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod> para obter instruções sobre como criar um segredo de extração de imagem para uso com o IBM Helm Chart Repository e IBM Entitled Registry.

Antes de começar:

- Assegure-se de que o espaço de nomes do produto baas exista emitindo o seguinte comando:

```
kubect1 get namespace baas
```

- Se o espaço de nomes baas não existir, emita o comando a seguir para criá-lo:

```
kubect1 create namespace baas
```

Para criar um segredo de extração de imagem para o registro Docker:

1. Emita o seguinte comando para criar o segredo de extração de imagem:

```
kubectl create secret docker-registry secret_name --namespace namespace_name --docker-server=registry_name --docker-username=docker_user or "token" --docker-password=password/token --docker-email=email
```

2. Determine os espaços de nomes de quaisquer PVCs de volume persistente que você deseja proteger emitindo o seguinte comando:

```
kubectl get pvc --all-namespaces
```

3. Para cada PVC que você deseja proteger, copie o segredo para esse espaço de nomes da PVC. Por exemplo, para copiar o segredo `baas-registry-secret` que você criou para o espaço de nomes `baas` no espaço de nomes `namespace1`, emita o seguinte comando:

```
kubectl get secret "baas-registry-secret" --namespace="baas" --export -o yaml | kubectl apply --namespace="namespace1" -f -
```

Instalando e implementando imagens do Suporte de Backup de Kubernetes no ambiente de Kubernetes

Antes de fazer backup e restaurar volumes persistentes anexados aos seus contêineres em um ambiente de cluster de Kubernetes, você deve instalar e implementar imagens do Suporte de Backup de Kubernetes.

Antes de Iniciar

É possível instalar o Kubernetes Backup Support usando um dos métodos a seguir:

Fazendo o download e instalando o pacote Helm do IBM Helm Charts Repository e IBM Entitled Registry

O pacote Helm é menor em tamanho e, portanto, leva menos tempo para download. O acesso à Internet é necessário para obter contêineres no momento da implementação. É possível fazer o download do arquivo de pacote Helm denominado `ibm-spectrum-protect-plus-prod-1.0.0.tgz` em <https://github.com/IBM/charts/tree/master/repo/entitled>.

Para obter instruções sobre a instalação do gráfico Helm, consulte o arquivo LEIA-ME do produto em <https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod>.

Fazendo o download e instalando o pacote do produto a partir do IBM Passport Advantage Online

O pacote de instalação do IBM Passport Advantage é um pacote maior, mas autocontido. O acesso à Internet não é necessário no momento da implementação. As instruções para download e instalação do pacote são fornecidas neste tópico.

Conclua as tarefas a seguir para fazer o download do pacote de instalação a partir do IBM Passport Advantage:

- Assegure-se de que seu ambiente de sistema atenda aos requisitos que estão descritos em “Requisitos do Suporte de Backup de Kubernetes” na página 54 e “Pré-requisitos para o Suporte de Backup de Kubernetes” na página 149.
- Faça o download do arquivo de instalação `SPP_V10.1.6_for_Containers.tar.gz` a partir do Passport Advantage® Online. Para obter informações sobre como fazer download de arquivos, consulte Nota técnica 5693313.
- Valide o arquivo transferido por download usando um dos métodos a seguir:
 - Verifique a soma de verificação MD5 do arquivo de instalação 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.
 - Verifique o arquivo assinado que está associado ao pacote de instalação emitindo o comando a seguir:

```
openssl dgst -sha256 -verify IBMSPSignCertificatePublic -signature ./SPP_V10.1.6_for_Containers.tar.gz.sig ./SPP_V10.1.6_for_Containers.tar.gz
```

Restrições:

- Um retrocesso para uma versão anterior do Suporte de Backup de Kubernetes não é suportado. Em outras palavras, não é possível usar o Suporte de Backup de Kubernetes V10.1.5 para restaurar dados que foram submetidos a backup pelo Suporte de Backup de Kubernetes V10.1.6.
- O upgrade do produto por meio do Suporte de Backup de Kubernetes V10.1.5 não é suportado.
- Devido a mudanças subjacentes no objeto BaasReq, não é possível usar Suporte de Backup de Kubernetes V10.1.6 para restaurar dados que foram submetidos a backup pelo Suporte de Backup de Kubernetes V10.1.5.

Sobre Esta Tarefa

Durante o procedimento de instalação e implementação, deve-se atualizar o arquivo de configuração `baas_config.cfg` com especificações para o seu ambiente e, em seguida, executar o script de instalação `baas_install.sh`. Ao executar o script de instalação, um gráfico do Helm apropriado é chamado automaticamente para implementar o Suporte de Backup de Kubernetes em seu ambiente.

Procedimento

Conclua as etapas a seguir na linha de comandos no ambiente de Kubernetes:

1. Efetue login no cluster de destino como um usuário com privilégios `cluster-admin`.
2. Descompacte o pacote de instalação (`SPP_V10.1.6_for_Containers.tar.gz`) inserindo o comando a seguir:

```
tar -xvf SPP_V10.1.6_for_Containers.tar.gz
```

Esse comando extrai uma pasta que é denominada `installer`.

3. Acesse o diretório `installer` inserindo o seguinte comando:

```
cd installer
```

4. Execute o comando a seguir para obter o método CIDR (Classless Inter-Domain Routing) para o cluster. Os valores são usados na Etapa “6” na página 154.

```
kubectl cluster-info dump | grep -m 1 cluster-cidr
```

O CIDR é fornecido na saída no formato a seguir:

```
--cluster-cidr=xxx.yyy.0.0/zz
```

Dica: Se o comando não retornar o CIDR, mude a expressão **grep** para procurar a combinação de "cluster" e "CIDR" e execute o comando novamente.

O CIDR é semelhante ao exemplo a seguir:

```
198.51.0.0/24
```

5. Execute o seguinte comando para obter o cluster e o endereço IP e porta para o servidor de API do cluster. Os valores são usados na Etapa “6” na página 154.

```
kubectl config view|awk '/cluster\:\/\/,server\:\/\/' | grep server\: | awk '{print $2}'
```

O resultado é uma URL que é composta por um endereço IP e um número de porta, conforme mostrado no exemplo a seguir:

```
https://192.0.2.0:6443
```

em que `192.0.2.0` é o endereço IP do servidor da API do cluster e `6443` é o endereço da porta.

6. Edite o arquivo `baas_config.cfg` com um editor de texto e modifique os parâmetros de configuração, fornecendo os valores apropriados para o seu ambiente. Coloque os valores entre aspas, conforme mostrado no exemplo a seguir.

```
BAAS_ADMIN="sppadmin"
```

A tabela a seguir contém os parâmetros que você deve modificar:

Tabela 54. Especificações para o arquivo de configuração <code>baas_config.cfg</code>	
Parâmetro	Descrição
BAAS_ADMIN	O ID do usuário do administrador do IBM Spectrum Protect Plus .
BAAS_PASSWORD	A senha do IBM Spectrum Protect Plus. Para maior segurança, especifique uma sequência vazia (" "). É solicitado que você forneça uma senha ao executar o script de implementação. Se você precisar especificar uma senha no arquivo de configuração para implementações de teste automatizadas, assegure-se de que o arquivo esteja armazenado em um local seguro.
CLUSTER_NAME	O nome do cluster exclusivo que é usado para registrar o host do aplicativo para o servidor IBM Spectrum Protect Plus.
CLUSTER_CIDR	O CIDR para o cluster. Insira o CIDR que foi obtido na Etapa “4” na página 153.
CLUSTER_API_SERVER_IP_ADDRESS	O endereço IP ou o nome completo do domínio (FQDN) para o servidor de API do cluster. Insira o endereço IP ou FQDN que foi obtido na Etapa “5” na página 153.
CLUSTER_API_SERVER_PORT	O endereço de porta para o servidor de API do cluster. Digite o endereço de porta que foi obtido na Etapa “5” na página 153.
LICENSE	A licença do produto para Suporte de Backup de Kubernetes. O arquivo de licença em inglês está localizado no diretório <code>installer/licenses/LA_en</code> que está incluído no pacote de instalação. As versões da licença em outros idiomas estão disponíveis em Documentos de Informações sobre a Licença . Revise as informações da licença e especifique <code>ACCEPT</code> para aceitar a licença durante a instalação sem ser perguntado. O valor padrão é <code>NOTACCEPTED</code> . Se você não alterar o valor padrão, será solicitado que você aceite a licença durante a instalação. Caso contrário, a instalação falhará.
SPP_AGENT_SERVICE_NODEPORT	A porta SSH para a conexão de IBM Spectrum Protect Plus a partir do serviço de contêiner do agente Suporte de Backup de Kubernetes. Se você não especificar um valor para essa porta, uma porta aleatória dentro do intervalo NodePort é designada pelo serviço NodePort em Kubernetes. O intervalo padrão é 30000 - 32767. Se você especificar um valor para essa porta, use um número de porta dentro do intervalo NodePort configurado pelo administrador de Kubernetes. Assegure-se de que a porta ainda não esteja em uso pelo cluster. Se a porta já estiver em uso, o processo de instalação falhará com um erro que mostra quais NodePorts já estão em uso.
SPP_IP_ADDRESSES	O endereço IP ou FQDN do servidor IBM Spectrum Protect Plus.

Tabela 54. Especificações para o arquivo de configuração <i>baas_config.cfg</i> (continuação)	
Parâmetro	Descrição
PRODUCT_IMAGE_REGISTRY	O endereço de registro do Docker e a porta que hospeda os contêineres. Insira o endereço no formato <i>ip_address:port</i> .
PRODUCT_IMAGE_REGISTRY_NAMESPACE	O espaço de nomes de registro Docker que hospeda os contêineres.
PRODUCT_IMAGE_REGISTRY_SECRET_NAME	O nome do segredo de extração de imagem do Kubernetes que contém as credenciais para o registro. O segredo deve estar no namespace que é especificado pelo parâmetro PRODUCT_IMAGE_REGISTRY_NAMESPACE. Se você estiver usando um registro interno, insira uma sequência vazia (""). Para que o contêiner do movedor de dados seja executado, o segredo de extração de imagem deve estar em cada espaço de nomes de cada solicitação de volume persistente (PVC) para ser submetido a backup e restaurado. Para obter instruções sobre como criar o segredo imagem-pull, consulte “Criando um segredo de extração de imagem para usar com um registro externo” na página 151 .
PRODUCT_LOGLEVEL	Os níveis de rastreamento para resolução de problemas com os componentes de gerenciador de transações, controlador e planejador do Suporte de Backup de Kubernetes. Os níveis de rastreamento a seguir estão disponíveis: INFO, WARNING, DEBUG ou ERROR. Padrão: INFO

Restrições:

- Os parâmetros e valores a seguir são reservados para Suporte de Backup de Kubernetes. Mantenha-os como estão.

```
PRODUCT_NAMESPACE="baas"
OPERATOR_NAMESPACE="default"
PRODUCT_TARGET_PLATFORM="K8S"
```

- O valor SPP_PORT especifica a porta para a interface com o usuário do IBM Spectrum Protect Plus. Não altere o valor padrão de 443.
- Suporte de Backup de Kubernetes está disponível apenas em inglês em IBM Spectrum Protect Plus V10.1.6. Por essa razão, não altere a configuração PRODUCT_LOCALIZATION="en_US".

Suas especificações são automaticamente inseridas no ConfigMap (baas-configmap) durante a implementação.

- Inicie a instalação e a implementação emitindo o comando a seguir.

```
./baas_install.sh -i
```

Quando solicitado, insira sim para continuar.

- Durante o processo de instalação, é solicitado que você forneça as seguintes informações:
 - Insira o ID e a senha de administrador do IBM Spectrum Protect Plus quando solicitado.
 - Quando solicitada a verificação da conectividade com o servidor IBM Spectrum Protect Plus, digite yes para continuar.

Se você inserir no, a instalação continua sem verificar a conectividade com o servidor IBM Spectrum Protect Plus.

Se você digitar yes e o teste de conectividade falhar, a instalação será finalizada com a seguinte mensagem de erro:

```
ERROR: Could not connect to IBM Spectrum Protect Plus server with provided credentials.
```

Dependendo do seu ambiente, pode levar vários minutos para o carregamento e a implementação do pacote.

9. Para verificar se os componentes do Suporte de Backup de Kubernetes estão devidamente instalados, emita o comando a seguir:

```
./baas_install.sh -s
```

Se a instalação falhar, os componentes ausentes serão listados na seção MISSING da saída.

Dica: Também é possível verificar o status da instalação com o comando **./helm status baas**.

Resultados

Quando todos os pods estiverem em execução, a implementação será concluída. Para verificar se todos os pods estão no estado Running e nenhum componente está ausente, emita o comando a seguir:

```
kubectl get pods -n baas
```

ou

```
kubectl describe pod pod_name -n baas
```

A saída é semelhante ao seguinte exemplo:

```
kubectcl get pods -n baas
NAME                                READY   STATUS    RESTARTS   AGE
baas-controller-768869468c-crt4d4   1/1     Running   0           4m24s
baas-kafka-68d7ff8455-m96cc         1/1     Running   0           4m24s
baas-scheduler-656978d87f-thqv2     1/1     Running   1           4m24s
baas-spp-agent-cdb784466-v9tnz      1/1     Running   0           4m24s
baas-transaction-manager-657db7bb8b-6dgqb 1/1     Running   2           4m24s
-----
All pods are running.
All resources are installed successfully.
A instalação foi concluída.
Product release >>baas<< version 10.1.6 has been isntalled in namespace >>baas<< at Wed May 20
17:58:02 MST 2020.
Script baas_install.sh finished at Wed May 20 17:58:02 MST 2020. A log of this transaction has
been written to /tmp
/baas_installation.sh_20200520-175605.log .
```

Se o contêiner do movedor de dados não estiver listado na saída, ele será implementado no tempo de execução.

É possível mostrar os serviços do Suporte de Backup de Kubernetes que estão configurados emitindo o seguinte comando:

```
kubectl get services -n baas
```

A saída é semelhante ao seguinte exemplo:

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
baas-kafka-svc	ClusterIP	10.110.116.210	<none>	9092/TCP,2181/TCP	4m27s
baas-scheduler	ClusterIP	10.96.38.170	<none>	8000/TCP	4m27s
baas-spp-agent	NodePort	10.110.164.151	<none>	22:30412/TCP	4m27s
baas-transaction-manager	ClusterIP	10.108.42.194	<none>	5000/TCP	4m27s

O serviço baas-datamover é implementado no tempo de execução com o tipo NodePort em vez de o intervalo ClusterIP com o protocolo TCP.

É possível mostrar as políticas de rede do Suporte de Backup de Kubernetes que estão implementadas emitindo o seguinte comando:

```
kubectyl get networkpolicies -n baas
```

A saída é semelhante ao seguinte exemplo:

NAME	POD
baas-ctl-networkpolicy	app.kubernetes.io/component=controller,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-kafka	app.kubernetes.io/component=kafka,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-scheduler	app.kubernetes.io/component=scheduler,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-spp-agent	app.kubernetes.io/component=spp-agent,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-transaction-manager	app.kubernetes.io/component=transaction-manager,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6

A política de rede para o movedor de dados é implementada no tempo de execução com o pod-seletor `app.kubernetes.io/name=baas,app.kubernetes.io/component=datamover,version=10.1.6`.

O que Fazer Depois

Após a conclusão da implementação, o host do aplicativo para o contêiner do Suporte de Backup de Kubernetes é registrado automaticamente na inicialização do host de cluster em Kubernetes. No entanto, se o registro automático foi malsucedido, é possível registrar manualmente o cluster usando a interface com o usuário do IBM Spectrum Protect Plus. Para obter instruções, consulte [“Registrando um cluster de Kubernetes” na página 322](#).

Se quiser atualizar a configuração existente ou fazer upgrade de uma instalação existente do Suporte de Backup de Kubernetes, modifique os parâmetros no arquivo `baas_config.cfg` conforme necessário para seu ambiente e emita o seguinte comando:

```
./baas_install.sh -u
```

Conceitos relacionados

[“Resolução de Problemas do Suporte de Backup de Kubernetes” na página 534](#)

Para ajudar a solucionar problemas com Suporte de Backup de Kubernetes, é possível coletar arquivos de log de depuração e visualizar logs de rastreamento. Também é possível seguir procedimentos para diagnosticar problemas.

Tarefas relacionadas

[“Configurando o nível de rastreamento de arquivos de log” na página 535](#)

É possível configurar o nível de rastreamento de arquivos de log locais para ajudar a solucionar problemas que você pode encontrar no Suporte de Backup de Kubernetes.

Desinstalando o Suporte de Backup de Kubernetes

É possível desinstalar completamente o Suporte de Backup de Kubernetes para que todos os componentes, incluindo todas as configurações e backups, sejam removidos do ambiente de Kubernetes.

Antes de Iniciar

Tome as ações a seguir antes de iniciar a desinstalação:

- Pare todos os backups planejados. Para obter instruções, consulte [Descontinuando backups de SLA para uma PVC ou Modificando parâmetros em um arquivo YAML](#).
- Aguarde todas as tarefas de backup e restauração em execução serem concluídas.

Procedimento

Para desinstalar completamente o Suporte de Backup de Kubernetes do cluster no qual você está logado, conclua as etapas a seguir na linha de comandos:

1. Destrua todos os backups de captura instantânea e cópia com uma solicitação **destroy**. Para obter instruções, consulte [“Excluindo backups de contêiner”](#) na página 353.
2. Exclua quaisquer solicitações de volume persistente (PVCs) que foram usadas para backups de cópias.

Dica: Você pode procurar os nomes das PVCs que foram submetidas a backup.

3. Exclua a definição de recurso customizada (CRD) baas emitindo o comando a seguir:

```
kubect1 delete crd baasreqs.baas.io
```

Esse comando também exclui todos os objetos de solicitação BaasReq.

4. Desinstale o Suporte de Backup de Kubernetes emitindo o seguinte comando do diretório `installer`:

```
./baas_install.sh -d
```


Quando solicitado, insira `sim` para continuar.

Esse comando remove todos os pods do movedor de dados, implementações e políticas de rede. O segredo de Kubernetes para Suporte de Backup de Kubernetes também é removido.


5. Opcional: Para verificar o progresso da desinstalação, digite o comando a seguir:

```
kubect1 get pod -n baas
```

6. Cancele o registro do cluster de Kubernetes usando a interface com o usuário do IBM Spectrum Protect Plus:

- a) Na área de janela de navegação, clique em **Gerenciar proteção > Contêineres > Kubernetes**.
- b) Na página **Kubernetes**, clique em **Gerenciador de Clusters**.
- c) Na lista de endereços do host, clique no ícone de exclusão  próximo do cluster do qual deseja cancelar o registro.
- d) Na janela **Confirmar**, insira o código de confirmação exibido e clique em **Cancelar registro**.

7. Remova a identidade da conta que é usada para registrar o cluster de Kubernetes:

- a) Na área de janela de navegação, clique em **Contas > Identidade**.
- b) Clique no ícone de exclusão  que está associado ao cluster.
- c) Clique em **Sim** para excluir a identidade.

8. Desative o recurso **VolumeSnapshotDataSource** se ele não for mais necessário.

9. Exclua as políticas de acordo de nível de serviço (SLA) e quaisquer outras customizações excluindo o espaço de nomes baas. Emita o seguinte comando:

```
kubect1 delete namespace baas
```

10. Se você criou manualmente um segredo de extração de imagem para uso com um registro externo, remova o segredo com o comando **kubect1 delete secret** em todos os espaços de nomes em que o segredo existia.
11. Opcional: Revise as informações de instalação e de configuração e reverta quaisquer etapas de pré-requisito.

O que Fazer Depois

Se o Suporte de Backup de Kubernetes não foi perfeitamente desinstalado, consulte "Suporte de Backup de Kubernetes não foi perfeitamente desinstalado" em [“Resolução de problemas de referência rápida”](#) na página 537.

Capítulo 6. 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 copiar e restaurar dados, são discutidas em detalhes em outras áreas da documentação.

Antes de iniciar, assegure-se de que você tenha seguido 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 [“Storyboard de implementação para IBM Spectrum Protect Plus”](#) na [página 1](#) estejam 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.

Em seguida, as tarefas de backup e restauração de recursos são concluídas pelo *administrador do aplicativo*. No entanto, um único administrador pode ser responsável por todas as tarefas em seu ambiente.

Ação	Owner	Descrição
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	Descrição
“Gerenciar sites” na página 162	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 copiar 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 entidades que você deseja proteger. Depois que um recurso é registrado, um inventário do recurso é capturado e incluído no inventário IBM Spectrum Protect Plus.

Ação	Owner	Descrição
<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-SysXyz`. O usuário `serveradmin` é usado para acessar o console administrativo e o dispositivo virtual IBM Spectrum Protect Plus. A senha para `serveradmin` deve ser alterada antes de acessar o console administrativo e o dispositivo virtual IBM Spectrum Protect Plus.

As regras a seguir são impostas ao criar uma nova senha:

- O comprimento mínimo de senha aceitável é de 15 caracteres.
- Deve haver oito caracteres na nova senha que não estejam presentes na senha anterior.
- A nova senha deve conter pelo menos um caractere de cada uma das classes (números, letras maiúsculas, letras minúsculas e outras).

- O número máximo de caracteres consecutivos idênticos que são permitidos na nova senha é de três caracteres.
- O número máximo de classes de caracteres consecutivos idênticos que são permitidas na nova senha é de quatro caracteres.
- 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

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 replicação do site e operações de cópia conforme descrito em “Incluindo um Site” na página 204. 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 replicação do site e operações de cópia conforme descrito em “Editando um Site” na página 205. d. Clique em Salvar.

Conceitos relacionados

[“Componentes do Produto” na página 6](#)

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 204](#)

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 (SLA), definem parâmetros que são aplicados a tarefas de backup. Estes parâmetros incluem a frequência e a retenção de backups.

Sobre Esta Tarefa

IBM Spectrum Protect Plus inclui políticas de SLA padrão, conforme descrito em [Capítulo 9, “Gerenciando Políticas SLA para Operações de Backup”](#), na página 233. É possível usar as políticas padrão, já que elas são ou modificam as políticas. Também é possível criar políticas de SLA customizadas.

Por exemplo, as etapas a seguir mostram como criar uma política de SLA para VMware. Esta tarefa não inclui instruções para ativar a replicação para servidores vSnap ou para copiar dados para o armazenamento de backup secundário, que são recursos opcionais. Para obter informações sobre como configurar esses recursos na política de SLA, consulte [“Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos”](#) na página 236.

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

Procedimento

Para criar uma política de SLA, 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 SLA** é exibida.
3. No campo **Nome**, insira um nome que forneça uma descrição significativa da política de SLA.
4. Clique em **Sistemas de arquivos VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB e Windows**.
5. Na seção **Política de backup**, configure as opções a seguir 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 que são criadas sem um planejamento podem ser executadas on demand.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de backup. Escolha entre **Minutos**, **Horas**, **Dias**, **Semanas**, **Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

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

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

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.

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

The screenshot shows the 'Policy Overview' form for creating a new SLA Policy. The form is titled 'New SLA Policy' and has a dark blue header. The 'Name' field is set to 'Copper'. Under the 'Platform' section, the first option is selected: 'VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB, Catalog, and Windows File Systems'. Other options are 'Kubernetes' and 'Amazon EC2'. The 'Backup Policy' section includes a 'Retention' of 1 month, a 'Frequency' of 3 days, a 'Start Time' of 06/02/2020 at 00:00 in the America/Los_Angeles timezone, and a 'Target Site' of Primary. There are checkboxes for 'Disable Schedule', 'Only use encrypted disk storage.', and 'Replication Policy' (Backup Storage Replication). At the bottom, there are 'Cancel' and 'Save' buttons.

Policy Overview

New SLA Policy

Name: Copper

☒ VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB, Catalog, and Windows File Systems

☐ Kubernetes

☐ Amazon EC2

Backup Policy

Retention: 1 Months

☐ Disable Schedule

Frequency: 3 Days

Start Time: 06/02/2020 00:00 America/Los_Angeles

Target Site: Primary

☐ Only use encrypted disk storage.

Replication Policy

☐ Backup Storage Replication

Cancel Save

Figura 12. Criando uma política de SLA

6. Clique em **Save**. A política de SLA agora pode ser aplicada a definições de tarefa de backup, conforme mostrado em [“Incluir recursos em uma definição de tarefa”](#) na página 169.

Conceitos relacionados

[“Replicar dados de armazenamento de backup”](#) na página 11

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.

[“Copiar capturas instantâneas para armazenamento de backup secundário” na página 11](#)

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 copiar capturas instantâneas de um servidor vSnap para o armazenamento de backup secundário.

[“Gerenciando Políticas SLA para Operações de Backup” na página 233](#)

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 de replicar ou copiar 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 de usuário para um administrador que possa executar operações de backup e restauração para os recursos 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 526](#).

Para criar funções de usuário customizado e grupos de recursos, consulte [“Criando um Grupo de Recursos” na página 518](#) e [“Criando uma função” na página 523](#)

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**.

User

Add User - User Information and Role

Select the type of user or group you want to add. Individual new user

Username vmadmin
Username must not be 'root', 'admin' or 'test'.

Password Show
Password must contain at least 8 characters.

ASSIGN ROLE

- ☐ Application Admin
- ☐ Backup Only
- ☐ Restore Only
- ☐ SYSADMIN
- ☐ Self Service
- ☒ VM Admin

PERMISSION GROUPS

- > Certificate
- > Cloud

Cancel Continue >

Figura 13. 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 14. Selecionando um grupo de recursos para a conta do usuário

8. Clique em **Criar usuário**.

Conceitos relacionados

[“Gerenciando o acesso de”](#) na página 517

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 entidades 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 nas seções a seguir:

- [Capítulo 10, “Protegendo sistemas virtualizados”, na página 249](#)
- [Capítulo 11, “Protegendo sistemas de arquivos”, na página 299](#)
- [Capítulo 12, “Protegendo os contêineres”, na página 317](#)
- [Capítulo 13, “Proteger dados em sistemas em nuvem”, na página 357](#)
- [Capítulo 14, “Protegendo bancos de dados”, na página 363](#)

Procedimento

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

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > 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 SLA

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

O exemplo a seguir mostra campos preenchidos.

Figura 15. Incluindo uma Instância do vCenter Server

5. Clique em **Save**.

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 SLA.

Sobre Esta Tarefa

Para propósitos de exemplo, esta tarefa descreve como selecionar uma política de SLA para recursos que estão em um VMware vCenter.

Procedimento

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

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > 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:

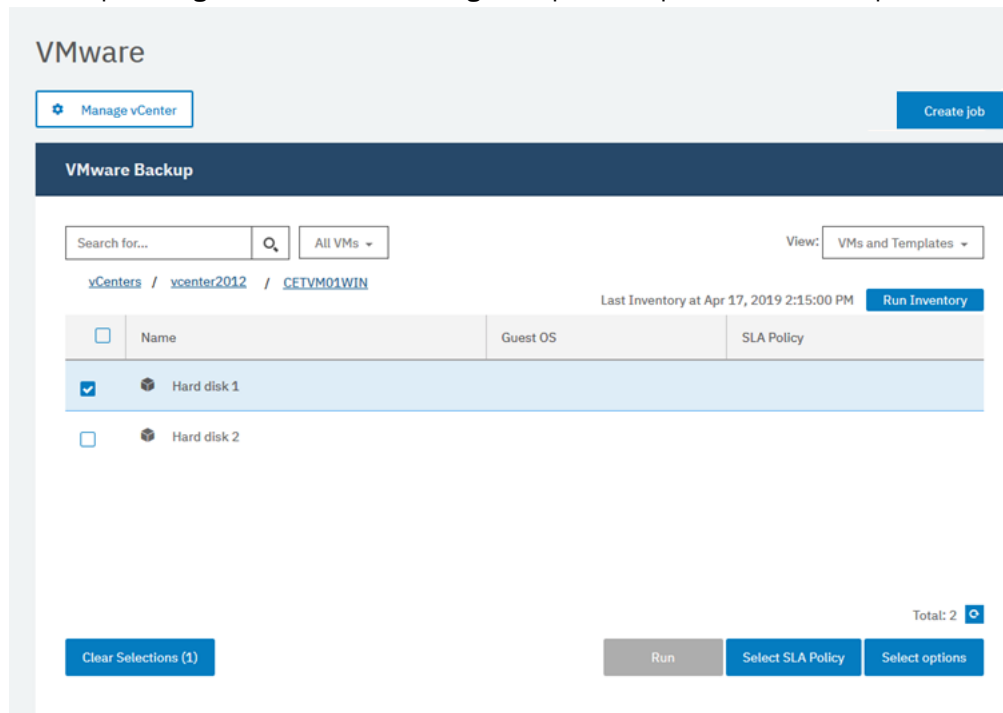


Figura 16. Selecionando recursos para backup

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

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

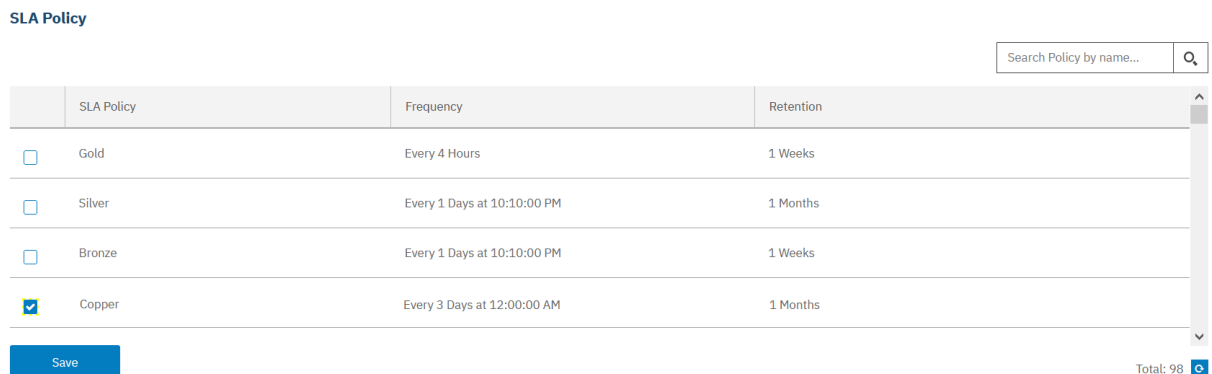


Figura 17. Selecionando uma política de SLA

4. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.
O nome da tarefa é gerado automaticamente e é construído do tipo de recurso seguido pela política de SLA que é usada para a tarefa. Para essa tarefa de exemplo, o nome vmware_Copper é criado.
5. Opcional: Para configurar opções adicionais, clique em **Selecionar opções** e siga as instruções em [“Fazendo backup dos dados de VMware” na página 253](#).
6. Clique **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 SLA que a máquina virtual. Opcionalmente, para definir uma política mais granular ao excluir VMDKs individuais, siga as instruções em [“Excluindo VMDKs da política de SLA para uma tarefa” na página 258](#).

Resultados

A tarefa é executada conforme definido pelas políticas de SLA 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 171.

Conceitos relacionados

[“Protegendo IBM Spectrum Protect Plus”](#) na página 491

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 e informações de tarefas são submetidas a backup em um servidor vSnap que é definido na política de SLA 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**.

Se sua tarefa não for uma tarefa planejada, mas uma tarefa on demand, clique na guia **Histórico de Tarefas**.

2. Escolha a tarefa que você deseja executar e clique na ação **Iniciar** conforme mostrado no exemplo a seguir:

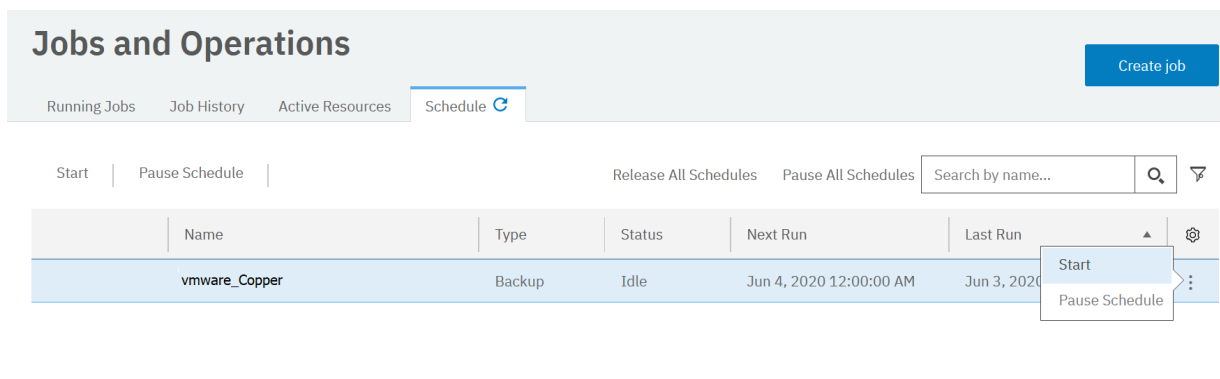


Figura 18. Iniciando uma Tarefa

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

[“Gerenciando tarefas e operações”](#) na página 495

É possível gerenciar e monitorar tarefas na janela **Tarefas e Operações**. Também é possível configurar scripts para serem executados antes ou depois de tarefas.

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. Clique na guia **Relatórios**.

Reports

Reports


Custom Reports

Filter by category

All

	Name (job title)	Category	Schedule
	Configuration	System	
	Container Persistent Volume Backup History	Protection	
	Container Persistent Volume Backup Utilization	Backup Storage Utilization	
	ContainerSLARPOComplianceDisplayName	Protection	
	Database Backup History	Protection	
	Database Backup Utilization	Backup Storage Utilization	
	Database SLA Policy RPO Compliance	Protection	
	Job	System	
	License	System	
	Protected and Unprotected Container Persistent Volumes	Protection	
	Protected and Unprotected Databases	Protection	
	Protected and Unprotected VMs	Protection	
	VM Backup History	Protection	
	VM Backup Utilization	Backup Storage Utilization	
	VM Datastores	VM Environment	
	VM LUNs	VM Environment	
	VM SLA Policy RPO Compliance	Protection	
	VM Snapshot Sprawl	VM Environment	
	VM Sprawl	VM Environment	
	VM Storage	VM Environment	
	vSnap Storage Utilization	Backup Storage Utilization	

Figura 19. Selecionando um relatório para execução

3. Execute o relatório clicando no ícone **Executar Relatório** () ao lado do relatório.
 - Para executar o relatório com parâmetros customizados, configure os parâmetros na janela **Executar relatório** 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 507](#)

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 7. 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 5693313](#).

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 491.
- 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.

Gerenciando Atualizações

Um ambiente do IBM Spectrum Protect Plus inclui o servidor IBM Spectrum Protect Plus, um ou mais servidores vSnap, e, opcionalmente, um ou mais proxies VADP. Para ajudar a garantir que o IBM Spectrum Protect Plus opere normalmente, todos os componentes no ambiente devem estar no mesmo nível de versão. Revise as instruções para planejar cuidadosamente e concluir o processo de atualização.

Antes de Iniciar

Execute as seguintes etapas:

1. Planeje um período de manutenção e verificação para o processo de atualização. É possível estimar o tempo necessário com base no número de componentes no ambiente que devem ser atualizados.

O processo de atualização de um ambiente do IBM Spectrum Protect Plus depende do número de componentes no ambiente e da velocidades de rede dos locais envolvidos. A tabela a seguir contém os três componentes do IBM Spectrum Protect Plus e o tempo médio, em minutos, que leva para aplicar a atualização e reiniciar o sistema com sucesso.

Tabela 55. Componentes do IBM Spectrum Protect Plus e tempos de upgrade

Componente	Tempo de atualização	Tempo de reinicialização	Total
IBM Spectrum Protect Plus Server	10	15	25
servidor vSnap	15	10 - 30	25 - 45
Servidor proxy VADP	15	Não necessário.	15

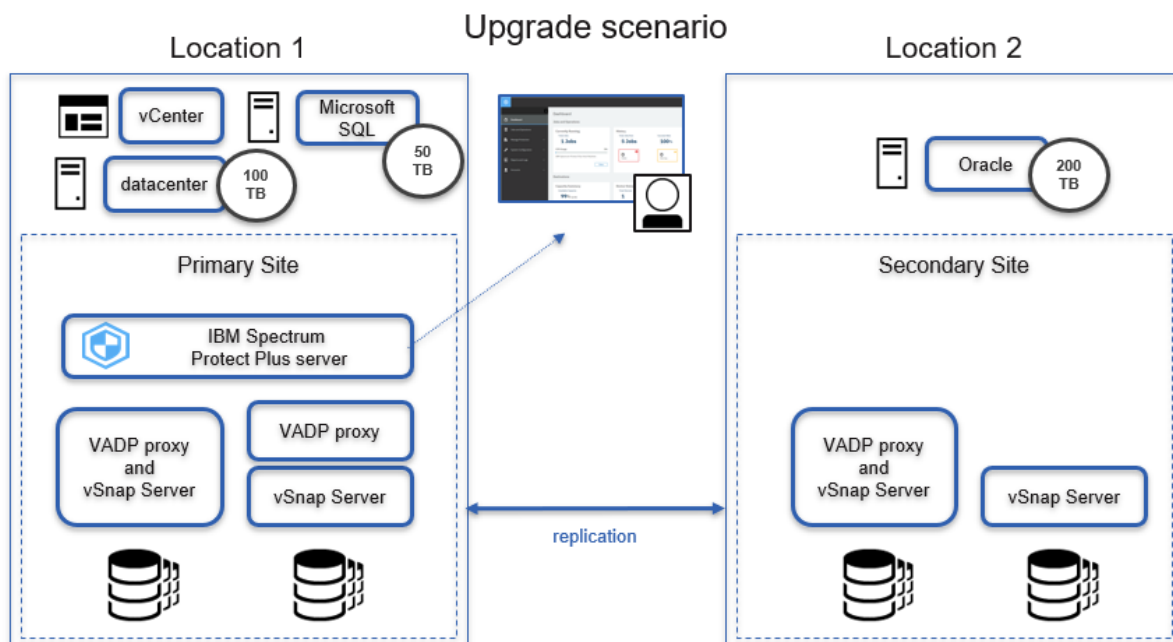
2. Reúna informações de versão para os componentes em seu ambiente e determine os níveis de versão para o processo de atualização. Determine se os servidores vSnap devem ser atualizados como parte do processo de upgrade.
3. Ajuste os horários de início das tarefas de inventário ou de manutenção planejadas para que elas sejam executadas após a conclusão do período de manutenção e verificação.
4. Finalize quaisquer tarefas de restauração ou reutilização, incluindo tarefas de restauração de armazenamento de objetos. Se necessário, planeje essas tarefas após a conclusão do período de manutenção e verificação.
5. Pause quaisquer tarefas restantes para que elas não sejam executadas durante o período de manutenção e verificação.

Sobre Esta Tarefa

O procedimento é baseado em um ambiente de exemplo, que inclui os componentes a seguir:

- 1 servidor IBM Spectrum Protect Plus
- 2 servidores vSnap integrados e 2 independentes, sendo que todos os 4 servidores têm relacionamentos de replicação
- 2 proxies VADP co-instalados com dois dos servidores vSnap
- 1 proxy VADP independente

Na figura a seguir, os componentes são exibidos em seus respectivos locais, Local 1 e Local 2:



Procedimento

1. Para preparar o ambiente do sistema para o processo de atualização, conclua as etapas a seguir:
 - a) Na área de janela de navegação, clique em **Gerenciar Proteção > Visão Geral de Política** e, em seguida, clique no botão **Incluir Política de SLA**.
 - b) Na área de janela **Nova Política de SLA**, digite um nome da política e clique no botão de opções que inclui a palavra **Catálogo**. Clique em **Salvar**.
 - c) Marque a caixa de seleção **Desativar Planejamento** e especifique um período de retenção apropriado. Na lista **Site de Destino**, selecione o site que conterá o backup do catálogo.
 - d) Opcionalmente, especifique outras opções para a tarefa de backup. Clique em **Salvar**.
 - e) Na área de janela de navegação, clique em **Gerenciar proteção > IBM Spectrum Protect Plus > Backup**.
 - f) Na área de janela **Política de SLA**, selecione a política que você criou. Clique em **Salvar**.
 - g) A política é exibida na área de janela **Status da Política de SLA**. Se ela não aparecer automaticamente, clique no botão atualizar.
 - h) Para iniciar o backup do catálogo, clique em **Ações** e, em seguida, clique em **Iniciar**.
 - i) Verifique a conclusão da tarefa de backup do catálogo. Na área de janela de navegação, clique em **Tarefas e Operações** para verificar se a tarefa de backup do catálogo foi concluída com sucesso.
 - j) Pausar todas as tarefas planejadas. Na área de janela de navegação, clique em **Tarefas e Operações** e clique na guia **Planejamento**. Clique em **Pausar todos os planejamentos**. O status para todas as tarefas planejadas será alterado para **Retido**.
 - k) Para verificar se nenhuma tarefa está em execução, clique na guia **Tarefas em Execução**. Se as tarefas estiverem em execução, permita que elas concluam o processamento.
2. Para preparar-se para a atualização de servidores vSnap, revise o IBM Spectrum Protect Plus Blueprints em <https://www.ibm.com/support/pages/node/1119489>. Cada servidor vSnap em seu ambiente deve ser atualizado para o mesmo nível de versão do IBM Spectrum Protect Plus. Para atualizar os servidores vSnap, conclua as seguintes etapas:
 - a) Siga as etapas para atualizar o sistema operacional para servidores vSnap, conforme descrito em [“Atualizando o sistema operacional para um servidor vSnap virtual”](#) na página 177.

Importante: Você deve renomear o arquivo ISO transferido por download conforme descrito no procedimento e mover o arquivo para o diretório /tmp no servidor vSnap se quiser atualizar o sistema operacional.
 - b) Conclua as etapas para atualização de um servidor vSnap, conforme descrito em [“Atualizando um servidor vSnap”](#) na página 178.

Dica: Depois que você atualizar um servidor vSnap, ele pode levar 15 minutos a mais do que em versões anteriores para reiniciar o servidor vSnap. Para obter mais informações, consulte <https://www.ibm.com/support/pages/node/3531159>.
3. Atualize o servidor IBM Spectrum Protect Plus concluindo as etapas a seguir:
 - a) Opcional: Se o servidor IBM Spectrum Protect Plus for implementado virtualmente, faça uma captura instantânea do dispositivo na interface de hypervisor apropriada.
 - b) Atualize o servidor IBM Spectrum Protect Plus. Siga as etapas 1 até 6 no tópico [“Atualizando o dispositivo virtual IBM Spectrum Protect Plus”](#) na página 178. Não libere o planejamento ou quaisquer tarefas que estejam retidas conforme indicado nas duas últimas etapas.
 - c) Efetue login novamente no servidor IBM Spectrum Protect Plus.
4. Atualize os proxies VADP. Depois de atualizar o servidor IBM Spectrum Protect Plus, os proxies VADP são atualizados automaticamente. No entanto, os proxies podem não ser atualizados imediatamente. Para atualizar os proxies VADP imediatamente, siga as etapas no tópico [“Atualizando proxies VADP”](#) na página 181.
5. Verifique se todos os componentes foram atualizados com sucesso concluindo as etapas a seguir:

- a) Usando a conta `serveradmin`, efetue login no console administrativo do IBM Spectrum Protect Plus. Siga as etapas em “Efetuando Login no Console Administrativo” na página 210.
 - b) Clique em **Gerenciamento de Produtos**. Na tabela, verifique se os itens a seguir têm o mesmo nível de versão: `spp-release`, `vsnap`, `vsnap-dist`, `vadp` e `vadp-dist`.
 - c) Efetue logout do console administrativo do IBM Spectrum Protect Plus.
 - d) Carregue a tela inicial do IBM Spectrum Protect Plus abrindo um navegador suportado e inserindo a seguinte URL:


```
https://hostname/
```

 em que *hostname* é o endereço IP da máquina virtual em que o aplicativo é implementado.
 - e) Verifique se a versão e a compilação na tela inicial correspondem ao `spp-release` que foi exibido na seção **Gerenciamento do Produto** do console administrativo.
 - f) Para verificar se uma tarefa de manutenção pode ser concluída com sucesso no ambiente atualizado, na área de janela de navegação, clique em **Tarefas e Operações > Planejar**. Clique no ícone de opções  ao lado da Tarefa de Manutenção e selecione **Iniciar**. Monitore o progresso da tarefa por meio da área de janela **Tarefas e Operações**.
6. Libere as tarefas planejadas e, opcionalmente, remova a captura instantânea. Execute as seguintes etapas:
- a) Libere todos os planejamentos. Na área de janela de navegação, clique em **Tarefas e Operações > Planejar**. Clique em **Liberar Todos os Planejamentos**.
 - b) Opcional: Se você fez uma captura instantânea do dispositivo virtual IBM Spectrum Protect Plus, é possível excluir a captura instantânea do servidor IBM Spectrum Protect Plus usando a interface do hypervisor. Siga as instruções na documentação do hypervisor.

O que Fazer Depois

Se necessário, reinicie quaisquer tarefas que foram interrompidas ou pausadas durante o período de manutenção e verificação.

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

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 23.

Para verificar a versão atual e o sistema operacional para os servidores vSnap, conclua as seguintes etapas:

1. Efetue login 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:

```
$ vsnap system info
```

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 178](#)

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

A atualização do sistema operacional do servidor vSnap com o arquivo ISO fornece a você as últimas correções e atualizações de segurança disponíveis. Se o sistema operacional for CentOS Linux versão 7.4 ou anterior, você deve atualizar o sistema operacional antes de atualizar o software do servidor vSnap. A atualização do sistema operacional é opcional para a versão 7.5 ou 7.6. Um arquivo ISO é transferido por download e usado para atualizar servidores vSnap virtuais.

Antes de Iniciar

Antes de iniciar o processo de atualização, assegure-se de ter feito backup do seu ambiente IBM Spectrum Protect Plus conforme descrito em [“Fazendo backup do aplicativo IBM Spectrum Protect Plus” na página 491](#). Para obter informações sobre a obtenção do arquivo ISO, consulte [“Atualizando o dispositivo virtual IBM Spectrum Protect Plus” na página 178](#).

Restrição: O ISO não deve ser usado se você estiver atualizando um servidor físico Red Hat Enterprise Linux. Ele deve ser usado apenas em implementações de OVA.

Procedimento

1. Faça o download do arquivo ISO `<part_number>.iso`. Mova o arquivo ISO para o diretório `/tmp` no servidor vSnap e renomeie o arquivo para `spp_with_os.iso`.

```
$mv <part_number>.iso /tmp/spp_with_os.iso
```

Importante: É fundamental renomear o arquivo ISO transferido por download conforme descrito nesta etapa e movê-lo para o diretório `/tmp` no servidor vSnap se você quiser atualizar o sistema operacional.

2. Prosiga com as instruções encontradas no tópico [“Atualizando um servidor vSnap” na página 178](#). Quando o arquivo `<part_number>.run` for executado, o instalador atualizará opcionalmente o sistema operacional se `/tmp/spp_with_os.iso` estiver presente.

Um dos dois cenários a seguir ocorrerá, dependendo da presença do arquivo ISO.

- Se o arquivo estiver presente, os pacotes do sistema operacional serão atualizados e, depois, o software vSnap será atualizado.
- Se o arquivo não estiver presente, uma mensagem será exibida:

```
File /tmp/spp_with_os.iso is not present, skipping update of OS packages.  
To update OS packages, download the ISO file to /tmp/spp_with_os.iso and rerun this  
installer.
```

Em seguida, o software vSnap é atualizado.

Uma vez que o instalador for concluído, o `/tmp/spp_with_os.iso` poderá ser excluído.

Tarefas relacionadas

[“Atualizando um servidor vSnap” na página 178](#)

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 491](#).
2. Faça o download do arquivo de atualização `<part_number>.run` do vSnap e copie-o para um local temporário no servidor do vSnap. Para obter informações sobre como fazer download de arquivos, consulte [Nota técnica 5693313](#).

Procedimento

Para atualizar um servidor vSnap, conclua as seguintes etapas:

1. Efetue login no servidor vSnap como o usuário `serveradmin`.
2. A partir do diretório em que o arquivo `<part_number>.run` está localizado, torne o arquivo executável emitindo o comando a seguir:

```
$ chmod +x <part_number>.run
```

3. Execute o instalador emitindo o seguinte comando:

```
$ sudo ./<part_number>.run
```

Como alternativa, instalações não interativas ou atualizações do vSnap podem ser iniciadas usando a opção `noprompt`. Quando esta opção for usada, o instalador do vSnap ignorará o prompt para respostas e assumirá uma resposta "sim" para os prompts a seguir:

- Contrato de licença
- Instalação ou atualização do kernel
- Reinicializar no término da instalação ou atualizar, se necessário

Para usar a opção `noprompt`, emita o comando a seguir. Observe o espaço deliberado tanto antes quanto depois dos traços duplos:

```
$ sudo ./<part_number>.run -- noprompt
```

Os pacotes vSnap são instalados.

4. Depois que os pacotes vSnap estiverem instalados, inicie a versão atualizada do servidor vSnap.
5. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.
Localize as tarefas que você pausou.
6. No menu **Ações** para as tarefas pausadas, selecione **Planejamento de liberação**.

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

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 491.
2. Para fazer atualizações off-line, faça o download da atualização de pré-requisito do IBM Spectrum Protect Plus denominada *<part_number>.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 5693313](#).

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 SUPERUSER, insira o nome do usuário e a senha do 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 logon como um usuário do sistema, insira a senha serveradmin. A senha padrão é sppDP758-SysXyz. É solicitado que mude esta senha durante o primeiro logon.

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**. É possível selecionar somente um arquivo de atualização por vez.

Importante: Deve haver pelo menos 4.2 GB de espaço em disco disponível no diretório /tmp do servidor IBM Spectrum Protect Plus.

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 176](#)

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.

Etapas adicionais para atualização de máquinas virtuais em ambientes de Réplica do Hyper-V

A partir do IBM Spectrum Protect Plus Versão 10.1.5, é possível proteger máquinas virtuais (VMs) que estão ativadas para usar o recurso de Réplica do Hyper-V.

IBM Spectrum Protect Plus processa os dados nas instâncias de origem e replicadas das VMs separadamente. Por exemplo, se uma VM denominada VM1 estiver no host do Hyper-V denominada Host1 e a VM for replicada para Host2, IBM Spectrum Protect Plus atribuirá os IDs VM1@Host1 e VM1@Host2 às VMs. Em seguida, é possível selecionar uma ou ambas as VMs para proteção de dados.

Considerações para VMs que são definidas em políticas de SLA existentes

Se atualizar IBM Spectrum Protect Plus, você pode ter que executar etapas adicionais para assegurar que a proteção de dados continue para VMs atualmente incluídas em políticas de acordo de nível de serviço (SLA).

Uma política de SLA pode incluir uma VM replicada *implicitamente* ou *explicitamente*. Você pode ser obrigado a atualizar a política de SLA ao atualizar para o IBM Spectrum Protect Plus V10.1.5 ou mais recente.

Um exemplo de política de SLA que inclui implicitamente uma VM replicada é um cenário no qual a política protege todas as VMs em Host1, que contém a MV VM1. VM1 é replicado para Host2. Neste cenário, uma mudança para a política de SLA não é necessária após a atualização do IBM Spectrum Protect Plus. A política de SLA cria um backup completo da instância de VM1 em Host2 e cria um novo backup completo da instância de VM1 em Host1. Os backups existentes de VM1 em Host1 que foram criados antes da atualização expirarão com base nas configurações de retenção de política de SLA.

Um exemplo de uma política de SLA que inclui explicitamente uma VM replicada é um cenário no qual a política protege VM1 em Host1 e VM1 é replicada para Host2. Neste cenário, você deve reincluir a instância da VM em cada host para a política de SLA depois de atualizar IBM Spectrum Protect Plus.

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 491.

Nota: Somente os proxies VADP registrados com IBM Spectrum Protect Plus serão atualizados. Se o proxy VADP não estiver registrado com IBM Spectrum Protect Plus, o componente VADP não será atualizado.

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 reticências **...** e selecione **Editar**. Selecione **Usar usuário existente** e escolha uma identidade digitada anteriormente em **Selecionar usuário** 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>Consulte “Fazendo backup dos dados de VMware” na página 253.</p> <p>Os proxies são indicados no log da tarefa por uma mensagem de log semelhante ao seguinte texto:</p> <p>Executar vmdkbackup remoto de MicroService: http://<proxy <i>nodename</i>, IP:<i>proxy_IP_address</i></p>

Tarefas relacionadas

“Criando proxies do VADP” na página 260

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 104

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 8. Configurando o ambiente do sistema

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.



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 copiar capturas instantâneas de um servidor vSnap para um sistema de armazenamento em nuvem ou um servidor de repositório.

Para obter informações sobre como copiar dados de captura instantânea para o armazenamento secundário, consulte [“Copiar capturas instantâneas para armazenamento de backup secundário” na página 11.](#)

Gerenciando o armazenamento em

É possível copiar dados de captura instantânea para armazenamento em nuvem para proteção de dados de longo prazo.

Configuração para copiar ou arquivar dados na nuvem

Se você estiver planejando copiar ou arquivar dados do IBM Spectrum Protect Plus para o armazenamento em nuvem para retenção de longo prazo ou para armazenamento de captura instantânea, deve-se configurar o armazenamento secundário.

Tarefas para configurar o armazenamento em nuvem

Você deve configurar o IBM Spectrum Protect Plus para operações de backup e restauração para o armazenamento em nuvem, conforme mostrado na Tabela 1.

Cenário do Usuário	Finalidade	Etapas
Armazene dados deduplicados e dados não deduplicados em um conjunto de armazenamentos de contêiner em nuvem e restaure os dados conforme necessário.	Copie dados para armazenamento em nuvem. Na primeira operação de cópia, é criada uma cópia de backup completa. As cópias subsequentes são incrementais.	<p>Escolha um dos seguintes provedores:</p> <ul style="list-style-type: none"> • “Incluindo o Armazenamento de objeto do Amazon S3” na página 184 • “Incluindo o IBM Cloud Object Storage como um provedor de armazenamento de backup” na página 185 • “Incluindo armazenamento em nuvem do Microsoft Azure como um provedor de armazenamento de backup” na página 187 • “Incluindo armazenamento de objeto compatível com S3” na página 188

Incluindo o Armazenamento de objeto do Amazon S3

Você pode incluir o Amazon Simple Storage Service (S3) como um provedor de armazenamento de backup no IBM Spectrum Protect Plus para habilitar operações de cópia para o armazenamento do Amazon 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 211](#).

Assegure-se de que os depósitos de armazenamento em nuvem sejam criados para os dados do IBM Spectrum Protect Plus. Para obter instruções sobre como criar depósitos, consulte [Documentação do Amazon Simple Storage Service](#).

Procedimento

Para incluir o armazenamento em nuvem do Amazon S3 como um provedor Object Storage de backup, conclua as etapas a seguir:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Armazenamento de objeto**.
2. Clique em **Incluir armazenamento de objeto**.
3. Na lista **Provedor**, selecione **Amazon S3**.
4. Preencha os campos no formulário **Registro do Object Storage**:

Nome

Insira um nome significativo que ajuda você 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 esta opção para selecionar uma chave inserida anteriormente para o armazenamento e, em seguida, selecione a chave na 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 no AWS Management Console.

Chave secreta

Insira a chave secreta AWS. As chaves secretas são criadas no AWS Management Console.

Ativar o Deep Archive

Opcionalmente, selecione esta opção para ativar a classe de armazenamento do Amazon S3 Glacier Deep Archive.

5. Clique em **Obter Depósitos** para conectar IBM Spectrum Protect Plus ao AWS para recuperar a lista de depósitos disponíveis.
6. Selecione o depósito que você planeja usar como destino de cópia.
Os campos **Depósito de armazenamento de objeto padrão** e **Depósito de armazenamento de objeto de archive** são exibidos.
7. No campo **Bucket de armazenamento de objeto padrão**, selecione um depósito para entregar como o destino de cópia.
8. Opcional: No campo **Bucket de armazenamento de objeto de archive**, selecione um recurso de armazenamento em nuvem para entregar 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 [“Copiar capturas instantâneas para armazenamento de backup secundário”](#) na página 11.
9. Selecione **Deep Archive** para registrar o Amazon S3 Glacier Deep Archive Buckets para arquivamento de longo prazo.
10. Clique em **Registrar** para concluir a operação.
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 SLA que é usada para a tarefa de backup.	Para criar uma política de SLA, consulte “Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos” na página 236. Para modificar uma política de SLA existente, consulte “Editando uma política de SLA” na página 247.

Incluindo o IBM Cloud Object Storage como um provedor de armazenamento de backup

Inclua o IBM Cloud Object Storage para ativar o IBM Spectrum Protect Plus para copiar dados para 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 211 e [“Incluindo um Certificado”](#) na página 212.

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](#).

Ao criar um depósito no IBM Cloud Object Storage (COS), certifique-se de que **Incluir Regra de Archive e Incluir Regras de Expiração** não sejam selecionadas ao criar depósitos para serem usados para cópia ou arquivo. Isso pode resultar em uma falha com o erro "o depósito tem um erro de configuração de ciclo de

vida não suportado" quando a tarefa tentar ser executada em IBM Spectrum Protect Plus. A opção **Incluir Política de Retenção** pode ser configurada para um depósito a ser usado para cópia, mas não deve ser configurado para um depósito que será usado para arquivamento.

O depósito Cold Vault de tipo só deve ser usado durante o arquivamento, já que é a opção de menor custo e é descrito como ideal para retenção de longo prazo de dados que serão acessados minimamente.

Ao incluir o IBM Cloud Object Storage (COS), o método para obter o acesso e a chave secreta dependerá do modelo de implementação. Se no local, as chaves podem ser obtidas no IBM COS Manager Console. Para IBM COS IaaS, as chaves são criadas quando uma conta de serviço é criada e pode ser obtida a partir do portal Softlayer. Se usar IBM COS (COS as a Service), a chave de acesso e secreta não será criada por padrão; quando uma conta de serviço for criada, marque a caixa **Incluir Credencial HMAC** e inclua `{"HMAC": true}` na área de texto **Incluir Parâmetros de Configuração Sequenciais**.

Procedimento

Para incluir o IBM Cloud Object Storage como um provedor de armazenamento de backup, conclua as etapas a seguir:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Armazenamento de objeto**.
2. Clique em **Incluir armazenamento de objeto**.
3. Na lista **Provedor**, selecione **IBM Cloud Object Storage**.
4. Preencha os campos na área de janela **Registro de armazenamento de objeto**:

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 é necessário se você estiver incluindo o IBM Cloud Object Storage público.

5. Clique em **Obter depósitos** e, em seguida, selecione um depósito para entregar como o destino de cópia.

Após os depósitos serem gerados, os campos **Bucket de armazenamento de objeto padrão** e **Bucket de armazenamento de objeto de archive** serão exibidos.

6. No campo **Bucket de armazenamento de objeto padrão**, selecione um depósito para entregar como o destino de cópia.
7. Opcional: No campo **Bucket de armazenamento de objeto de archive**, selecione um recurso de armazenamento em nuvem para entregar 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 [“Copiar capturas instantâneas para armazenamento de backup secundário” na página 11](#).
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 SLA que é usada para a tarefa de backup.	<p>Para criar uma política de SLA, consulte “Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos” na página 236.</p> <p>Para modificar uma política de SLA existente, consulte “Editando uma política de SLA” na página 247.</p>

Incluindo armazenamento em nuvem do Microsoft Azure como um provedor de armazenamento de backup

Inclua o armazenamento em nuvem Microsoft Azure para ativar o IBM Spectrum Protect Plus para copiar dados para o armazenamento Microsoft Azure Blob.

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 > Armazenamento de Objetos**.
2. Clique em **Incluir armazenamento de objeto**.
3. Na lista **Provedor**, selecione **Armazenamento de blob do Microsoft Azure**.
4. Preencha os campos na área de janela **Registro de armazenamento de objeto**:

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 entregar como o destino de cópia.

Após os depósitos serem gerados, os campos **Bucket de armazenamento de objeto padrão** e **Bucket de armazenamento de objeto de archive** serão exibidos.

6. No campo **Bucket de armazenamento de objeto padrão**, selecione um depósito para entregar como o destino de cópia.

7. Opcional: No campo **Bucket de armazenamento de objeto de archive**, selecione um recurso de armazenamento em nuvem para entregar 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 [“Copiar capturas instantâneas para armazenamento de backup secundário” na página 11](#).

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 SLA que é usada para a tarefa de backup.	<p>Para criar uma política de SLA, consulte “Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos” na página 236.</p> <p>Para modificar uma política de SLA existente, consulte “Editando uma política de SLA” na página 247.</p>

Incluindo armazenamento de objeto compatível com S3

Além de fazer backup de dados para o Amazon Simple Storage Service (S3) e o IBM Cloud Object Storage, você pode querer fazer backup de dados para outros provedores de armazenamento de objetos compatíveis com S3. Antes de fazer backup de dados em um ambiente de produção para qualquer outro armazenamento de objeto compatível com S3, assegure-se de que o armazenamento de objeto tenha sido validado para uso com IBM Spectrum Protect Plus.

Antes de Iniciar

Dica:

Para obter informações sobre provedores de armazenamento de objetos compatíveis, consulte a [nota técnica 108714](#).

Configure a chave que é necessária para o objeto de nuvem. Para obter instruções, consulte [“Incluindo uma chave de acesso” na página 211](#).

Assegure-se de que os depósitos de armazenamento em nuvem estejam disponíveis. Para obter mais informações sobre depósitos de armazenamento em nuvem, consulte a documentação para o provedor de armazenamento compatível com S3.

Procedimento

Para incluir o armazenamento em nuvem compatível com S3 como um destino de backup, conclua as etapas a seguir:

1. No menu de navegação, clique em **Configuração do sistema > Armazenamento de backup > Armazenamento de objeto**.
2. Clique em **Incluir armazenamento de objeto**.
3. A partir da lista **Provedor**, selecione **Armazenamento Compatível com S3**.
4. Preencha os campos na área de janela **Registro de armazenamento de objeto**:

Nome

Insira um nome significativo para ajudar a identificar o armazenamento em nuvem.

Terminal

Insira o terminal do armazenamento em nuvem.

Usar chave de acesso existente

Ative esta opção para selecionar uma chave inserida anteriormente para o armazenamento e, em seguida, selecione a chave na 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 identificar a chave.

Chave de acesso

Insira a chave de acesso compatível com S3. Para obter instruções sobre a obtenção de chaves de acesso, consulte a documentação para o provedor de armazenamento compatível com S3.

Chave secreta

Insira a chave secreta compatível com S3. Para obter instruções sobre a obtenção de chaves de acesso, consulte a documentação para o provedor de armazenamento compatível com S3.

Certificado

Selecione a opção apropriada para incluir um certificado para o armazenamento compatível com o S3:

Fazer Upload

Para fazer upload de um certificado, clique em **Procurar** para localizar e selecionar o certificado. Clique em **Upload**.

Copiar e colar

Insira um nome para o certificado e cole o certificado na área de texto. Clique em **Criar**.

Utilizar existente

Se um certificado existir, selecione-o na lista **Selecionar um Certificado**.

5. Clique em **Obter Depósitos** e, em seguida, selecione um depósito para servir de destino.
Após os depósitos serem gerados, os campos **Bucket de armazenamento de objeto padrão** e **Bucket de armazenamento de objeto de archive** serão exibidos.
6. No campo **Depósito de Armazenamento de Objeto Padrão**, selecione um depósito para servir de destino de backup.
7. Opcional: No campo **Bucket de armazenamento de objeto de archive**, selecione um recurso de armazenamento em nuvem para entregar 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 [“Copiar capturas instantâneas para armazenamento de backup secundário” na página 11](#).
8. Clique em **Registrar**.
O armazenamento em nuvem foi incluído na tabela de servidores em nuvem.

O que Fazer Depois

Depois de adicionar o armazenamento compatível com S3, complete a seguinte ação:


Ação	Como
Associar o armazenamento em nuvem à política de SLA que é usada para a tarefa de backup.	<p>Para criar uma política de SLA, consulte “Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos” na página 236.</p> <p>Para modificar uma política de SLA existente, consulte “Editando uma política de SLA” na página 247.</p>

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 > Armazenamento de objeto**.
2. Clique no ícone editar  que está associado a um provedor de armazenamento de objeto. A área de janela **Atualizar Object Storage** 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 SLA 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 > Armazenamento de objeto**.
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 copiar dados 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 copiar dados para fita, Servidor IBM Spectrum Protect Versão 8.1.8 ou mais recente é necessário.

Você pode optar por replicar os dados do IBM Spectrum Protect Plus que são copiados para o Servidor IBM Spectrum Protect para um servidor de destino. No entanto, IBM Spectrum Protect Plus não está ciente das operações de replicação do Servidor IBM Spectrum Protect subsequentes e não é possível restaurar os dados replicados do Servidor IBM Spectrum Protect de destino para o IBM Spectrum Protect Plus.

Configuração para copiar ou arquivar dados para IBM Spectrum Protect

Se você estiver planejando copiar ou arquivar dados do IBM Spectrum Protect Plus para um Servidor IBM Spectrum Protect, há três configurações possíveis. A escolha de qual configurar depende de qual cenário se aplica às suas necessidades de proteção de dados. Para cada cenário, há etapas que são necessárias nos ambientes IBM Spectrum Protect Plus e Servidor IBM Spectrum Protect para concluir a configuração.

Tarefas para a configuração do IBM Spectrum Protect

Você deve configurar o Servidor IBM Spectrum Protect para se comunicar com o servidor IBM Spectrum Protect Plus e para ativar solicitações de processo para operações de backup e restauração. O protocolo Amazon Simple Storage Service (S3) permite a comunicação entre dois servidores.

Cenário do Usuário	Finalidade	Etapas
Copiar para o armazenamento de objetos padrão quando você estiver executando cópias diárias ou menos frequentes para armazenamento de objetos padrão.	Copie dados para o armazenamento de objeto padrão. Na primeira operação de cópia, é criada uma cópia de backup completa. As cópias subsequentes são incrementais. A cópia de dados para o armazenamento de objetos padrão é útil caso você queira obter tempos de backup e de recuperação relativamente rápidos e não precise dos benefícios de proteção, custo e segurança a longo prazo oferecidos pelo armazenamento em fita.	Para copiar dados para o armazenamento de objeto padrão para o Servidor IBM Spectrum Protect, deve-se criar um conjunto de armazenamentos de contêiner em nuvem ou de contêiner de diretório e configurar o componente do agente de objeto do IBM Spectrum Protect. Incluir o agente de objeto é uma etapa obrigatória. Além de configurar o conjunto de armazenamento necessário, siga as etapas 2-4 listadas aqui .
Copiar para fita quando você estiver criando uma cópia completa semanal ou menos frequente de seus dados para o armazenamento em fita. Importante: O arquivamento de dados para fita não pode ser executado com frequência menor que uma vez por semana. Por essa razão, os dados arquivados não devem ser considerados uma cópia que seja útil para a recuperação de desastres.	Quando você copia dados para fita, uma cópia completa dos dados é criada no momento do processo de cópia. A cópia de dados para fita fornece benefícios extras de segurança. 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. No entanto, como a cópia para esses tipos de armazenamento requer uma cópia de dados completa, 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 copiar dados para fita, deve-se criar um conjunto de armazenamentos de contêiner em nuvem ou de contêiner de diretório para fita e um conjunto de armazenamento em cache de dados frios no Servidor IBM Spectrum Protect. Incluir o agente de objeto é uma etapa obrigatória. Siga as etapas 1-4 listadas aqui .

Cenário do Usuário	Finalidade	Etapas
Mistura de armazenamento de objeto padrão e cópia de longo prazo para fita	Proteja seus dados em backups incrementais no Servidor IBM Spectrum Protect, além de reter dados em fita para segurança de longo prazo.	Essa é uma combinação dos casos anteriores: os dados são armazenados em fita e os dados são armazenados em armazenamento de objetos padrão no Servidor IBM Spectrum Protect. Assim como configurar os conjuntos de armazenamento de dados necessários para ambos os cenários, a criação de um agente de objeto é obrigatória.

As quatro etapas necessárias para instalar e configurar a comunicação de transferência de dados entre IBM Spectrum Protect Plus e o Servidor IBM Spectrum Protect são as seguintes:

1. Se você estiver configurando conjuntos de armazenamento para copiar dados em fita, siga a Etapa 1. Crie conjuntos de armazenamentos no Servidor IBM Spectrum Protect usando o IBM Spectrum Protect Operations Center. Para obter instruções, consulte [“Etapa 1: criando um conjunto de armazenamento em fita e um conjunto de armazenamento em cache de dados frios para copiar dados para fita”](#) na página 193. Essa etapa é necessária apenas se você estiver definindo IBM Spectrum Protect para arquivamento com cópias executadas uma vez por semana ou com menos frequência.
2. Crie um domínio de política que aponte para o conjunto ou conjuntos de armazenamentos. O domínio de políticas define as regras que controlam os serviços de backup do IBM Spectrum Protect Plus. Para obter instruções, consulte [“Etapa 2: configurando um domínio de política de objeto”](#) na página 195.
3. Se você estiver copiando dados para um conjunto de armazenamento padrão ou para fita, deve-se incluir armazenamento de objeto padrão no Servidor IBM Spectrum Protect. Para obter instruções, consulte [“Etapa 3: configurando o armazenamento de objeto padrão”](#) na página 196.
4. Inclua um agente de objeto no Servidor IBM Spectrum Protect. O agente de objeto fornece um gateway entre o servidor IBM Spectrum Protect Plus e o Servidor IBM Spectrum Protect. Para obter instruções, consulte [“Etapa 4: incluindo um agente de objeto para copiar dados”](#) na página 199.
5. Para concluir a configuração, é necessário incluir um cliente de objeto no Servidor IBM Spectrum Protect. O cliente do objeto identifica o servidor IBM Spectrum Protect Plus e permite que ele armazene objetos no Servidor IBM Spectrum Protect. As mesmas credenciais das que você usou para IBM Spectrum Protect Plus são usadas para o cliente de objeto, que é o cliente de objeto que está associado ao domínio de política, conforme configurado na Etapa 2. Para obter instruções para configurar um cliente de objeto, consulte [“Etapa 5: incluindo e configurando um cliente de objeto para copiar de dados”](#) na página 200.

Dica: Como alternativa, insira o comando **DEFINE STGPOOL** para criar um conjunto de armazenamentos, conforme descrito nos tópicos a seguir:

O que fazer a seguir

1. Depois de concluir as tarefas necessárias para o armazenamento do IBM Spectrum Protect, deve-se incluir o Servidor IBM Spectrum Protect no IBM Spectrum Protect Plus. Para obter informações sobre como fazer isso, siga as instruções em [“Registrando um servidor de repositório como um provedor de armazenamento de backup”](#) na página 202.
2. Quando isso é feito, é possível criar uma política de SLA que define o Servidor IBM Spectrum Protect como o destino de armazenamento de backup. Para obter mais informações para ajudá-lo a escolher qual tipo de política você precisa, consulte [“Configuração para copiar ou arquivar dados para IBM Spectrum Protect”](#) na página 190

Etapa 1: criando um conjunto de armazenamento em fita e um conjunto de armazenamento em cache de dados frios para copiar dados para fita

Antes de poder copiar dados do IBM Spectrum Protect Plus para o Servidor IBM Spectrum Protect para fins de arquivamento, deve-se configurar um serviço de agente de objeto. Para arquivamento de longo prazo de dados, deve-se configurar um conjunto de armazenamento de dados frios. Se você não estiver planejando arquivar dados para fita no Servidor IBM Spectrum Protect, você pode pular esta etapa.

Sobre Esta Tarefa

Antes de iniciar, assegure-se de ter dimensionado as suas necessidades de armazenamento em cache frio usando a ferramenta de dimensionamento e os Blueprints. Para obter informações sobre como fazer isso, consulte o [Blueprints](#). Para obter links e vídeos mais úteis, consulte [“Storyboard de implementação para IBM Spectrum Protect Plus” na página 1](#).

Os dados do cliente de objeto especificados com um armazenamento S3 Glacier não são acessados com frequência. Para ativar a cópia desses dados, que muitas vezes são chamados de *dados frios*, para armazenamento em fita, os dados são gravados temporariamente em um conjunto de armazenamento que atende aos requisitos para tratamento de dados do objeto. Em seguida, os dados são movidos para o dispositivo de fita ou VTL. Esse conjunto de armazenamentos, chamado de *conjunto de armazenamentos de cache de dados frios*, é designado a um domínio de políticas de clientes de objetos. Apenas dados de clientes de objetos podem ser gravados ou restaurados a partir de um conjunto de armazenamentos de cache de dados frios.

Procedimento

Se você não estiver usando o Operations Center, será possível usar o comando **define stgpool**. O comando pode ser definido da seguinte forma:

```
define stgpool NAME  
stgtype=colddatacache
```

Nota: Para configurar conjuntos padrão para armazenamento de objetos, siga estas etapas, mas quando você definir o tipo de conjunto de armazenamentos, selecione Padrão.

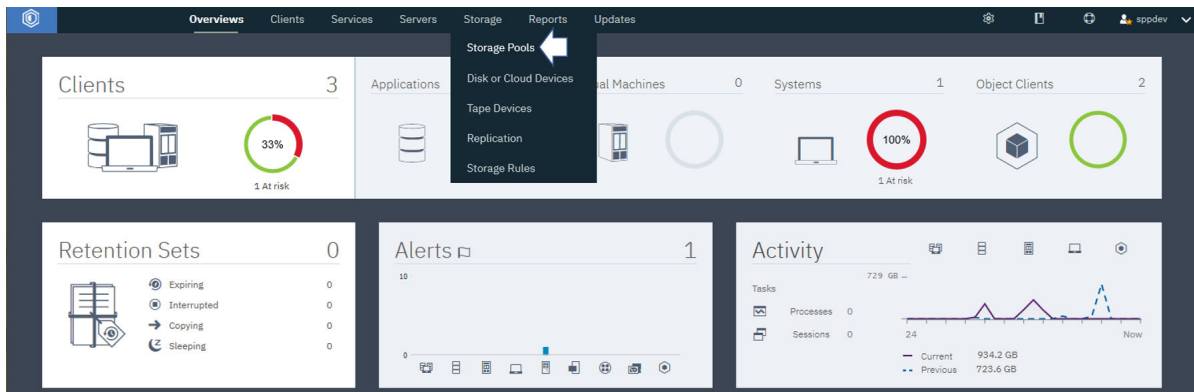
Para configurar o Servidor IBM Spectrum Protect para copiar dados de um cliente de objeto para a mídia de fita física ou um VTL, conclua as etapas de configuração a seguir:

1. No Servidor IBM Spectrum Protect, configure um conjunto de armazenamento primário que represente um dispositivo de fita ou VTL. Esse conjunto de armazenamento primário é o destino para os dados do objeto que você deseja copiar.

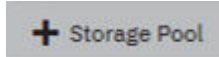
Posteriormente, ao definir o conjunto de armazenamentos de cache de dados frios, deve-se especificar esse conjunto de fitas como o próximo conjunto de armazenamentos para o conjunto de cache de dados frios.

Restrições: As restrições a seguir aplicam-se ao conjunto de armazenamento em fita:

- Não é possível replicar dados do cliente de objetos para ou a partir do conjunto de armazenamento em fita.
 - O conjunto de armazenamento em fita não pode ser deduplicado.
 - Não é possível especificar um próximo conjunto de armazenamentos para o conjunto de armazenamento em fita.
- a) Na barra de menus do Operations Center, clique em **Armazenamento > Conjuntos de armazenamentos**.



b) Na página **Conjuntos de Armazenamentos**, clique em **Conjunto de Armazenamentos**



c) No assistente **Incluir Conjunto de Armazenamentos**, selecione **Cliente do Objeto** para permitir que os clientes de objetos copiem dados para fita.

2. Execute as etapas do assistente para configurar um conjunto de armazenamento em cache de dados frios.

Um conjunto de armazenamento de cache de dados frios consiste em um ou mais diretórios do sistema de arquivos em disco. É um conjunto de armazenamento intermediário entre o cliente do objeto e um dispositivo de fita ou VTL e está vinculado ao conjunto de armazenamento de acesso sequencial primário que representa o dispositivo de fita ou VTL. Identifique um ou mais diretórios do sistema de arquivos existentes para armazenamento em disco temporário e o conjunto de armazenamento de acesso sequencial primário que representa o dispositivo de fita ou VTL.

3. Na página **Cache de Dados Frios**, especifique um ou mais diretórios do sistema de arquivos existentes para armazenamento em disco. Insira um nome de caminho completo que esteja em conformidade com a sintaxe usada pelo sistema operacional do servidor.

Por exemplo, digite `c:\temp\dir1\` para Microsoft Windows ou `/tmp/dir1/` para UNIX.

Os dados do objeto são armazenados em volumes sequenciais nos diretórios do sistema de arquivos. Um cliente de objeto pode copiar dados acessados com pouca frequência, ou dados frios, para a mídia de fita física ou para um VTL. Quando um cliente objeto copia dados frios, os dados são primeiramente armazenados no cache de dados frios. Em seguida, os dados são migrados, sem um atraso de migração, para o conjunto de armazenamento em fita primário que representa a mídia de fita física ou VTL. Depois que os dados são migrados para a fita, eles são excluídos do cache de dados frios. O cache de dados frios é usado como uma área temporária para restaurar dados frios para o cliente do objeto. Durante as operações de restauração, os dados são copiados para o cache de dados frios. Os dados permanecem no cache de dados frios por um período especificado pelo cliente objeto. Os dados são restaurados para o cliente do objeto do cache de dados frios e não diretamente da fita ou VTL.

Se você especificar vários diretórios para o aprimoramento de desempenho, assegure-se de que os diretórios correspondem a volumes físicos separados. Embora o cache de dados frios seja usado para armazenamento temporário, ele deve ser grande o suficiente para conter os dados que são copiados do cliente do objeto antes que os dados sejam migrados para a fita. Ele também deve ser grande o suficiente para manter dados durante as operações de restauração pelo período especificado pelo cliente objeto.

O que Fazer Depois

Ao concluir a configuração do conjunto de armazenamento em cache de dados frios, crie o domínio do objeto. Para obter instruções sobre como fazer isso, consulte [“Etapa 2: configurando um domínio de política de objeto” na página 195.](#)

Etapa 2: configurando um domínio de política de objeto

Antes de copiar dados de IBM Spectrum Protect Plus para o Servidor IBM Spectrum Protect, deve-se criar e configurar um domínio de política de objeto. O domínio de política define as regras que controlam os serviços de backup para IBM Spectrum Protect Plus. Você deve incluir um conjunto de armazenamento padrão que esteja com um diretório ou armazenamento baseado em contêiner em nuvem para cópias e um conjunto frio se você estiver copiando dados para fita ou arquivando dados.

Procedimento

1. Verifique as configurações do domínio de políticas que planeja utilizar para a cópia dos dados. Os clientes de objeto que são definidos ou atualizados no Servidor IBM Spectrum Protect V8.1.8 ou posterior devem ser designados a domínios de política que são criados com o comando **DEFINE OBJECTDOMAIN**. Um nó cliente de objeto é associado a esse domínio de política quando o nó é registrado ou atualizado com o comando **REGISTER NODE** ou **UPDATE NODE**.

Restrição: A partir do Servidor IBM Spectrum Protect V8.1.8, todos os novos nós clientes de objetos devem ser designados a domínios de políticas de objetos.

Para os nós clientes de objetos que foram designados a domínios de políticas de não objeto anteriores à V8.1.8, não é necessário atualizar a designação depois de fazer upgrade do servidor para o Servidor IBM Spectrum Protect V8.1.8. No entanto, caso seja necessário fazer alguma atualização no domínio do nó cliente de objeto, o nó deve ser designado a um domínio de políticas de objeto.

2. Revise as considerações a seguir para especificar domínios de políticas para operações de cópia.
 - Para o Servidor IBM Spectrum Protect, um domínio de políticas pode especificar classes de gerenciamento para conjuntos de armazenamentos padrão (conjuntos de armazenamentos de contêineres em nuvem ou de contêineres de diretório), conjuntos de armazenamentos de cache de dados frios ou para ambos os tipos de conjuntos de armazenamentos.

No entanto, para copiar dados do IBM Spectrum Protect Plus, deve-se especificar as classes de gerenciamento a seguir, que variam caso se esteja copiando dados para um conjunto de armazenamentos de contêineres em nuvem ou de contêineres de diretório ou copiando dados para um conjunto de armazenamentos de cache de dados frios para serem armazenados em uma mídia de fita física ou em uma Virtual Tape Library (VTL):

- Para copiar dados para um conjunto de armazenamentos de contêineres em nuvem ou de contêineres de diretório, use o parâmetro **STANDARDPOOL** para definir o conjunto de armazenamentos para o domínio de políticas, conforme mostrado no exemplo a seguir:

```
define objectdomain mydomain standardpool=hotpool
```

- Para copiar dados para um conjunto de armazenamentos de cache de dados frios, deve-se especificar um conjunto padrão e um conjunto frio para o domínio de políticas. O conjunto padrão é necessário para armazenar os metadados usados para as operações de restauração e outras operações do IBM Spectrum Protect Plus. Para definir um conjunto de armazenamentos de cache de dados frios para o domínio de políticas, use o parâmetro **COLDPOOL**, conforme mostrado no exemplo a seguir:

```
define objectdomain mydomain standardpool=hotpool coldpool=coldpool
```

- Todos os objetos são nomeados com exclusividade. Não há versões inativas de objetos. Ao definir um domínio de políticas, as políticas de Gerenciamento de armazenamento a seguir são especificadas automaticamente:
 - O campo `Versões de dados existentes` é configurado como 1.
 - Os campos `Reter versões adicionais` e `Reter apenas a versão` são configurados como 0.
- O servidor IBM Spectrum Protect Plus controla a hora em que os objetos são excluídos.

Exemplo: exibir informações detalhadas sobre um domínio de políticas para uma operação de cópia do IBM Spectrum Protect Plus

Quando o domínio de políticas é criado, são designadas classes de gerenciamento e grupos de cópias. É possível usar o comando **QUERY COPYGROUP** para visualizar informações sobre os conjuntos de armazenamentos de destino do domínio de políticas. No exemplo a seguir, o nome do domínio de políticas é XYZ. Os conjuntos de armazenamentos de destino são HOTPOOL e COLDPOOL.

```
query copygroup xyz standard f=d
```

```
Policy Domain Name: XYZ
Nome do Conjunto de Critérios: STANDARD
Mgmt Class Name: COLD
Nome do Grupo de Cópias: STANDARD
Tipo do Grupo de Cópias: Backup
Versions Data Exists: 1
Dados de Versões Eliminadas: 1
Retain Extra Versions: 0
Retain Only Version: 0
Modo de Cópia: Modified
Serialização de Cópias: Shared Static
Frequência de Cópias: 0
Copy Destination: COLDPOOL
Destino do Índice (TOC):
  Last Update by (administrator): SERVER_CONSOLE
  Last Update Date/Time: 05/22/20 17:03:46
  Perfil de Gerenciamento:
  Changes Pending: No

Policy Domain Name: XYZ
Nome do Conjunto de Critérios: STANDARD
Nome da Classe de Gerenciamento: STANDARD
Nome do Grupo de Cópias: STANDARD
Tipo do Grupo de Cópias: Backup
Versions Data Exists: 1
Dados de Versões Eliminadas: 1
Retain Extra Versions: 0
Retain Only Version: 0
Modo de Cópia: Modified
Serialização de Cópias: Shared Static
Frequência de Cópias: 0
Copy Destination: HOTPOOL
Destino do Índice (TOC):
  Last Update by (administrator): SERVER_CONSOLE
  Last Update Date/Time: 03/05/20 22:15:18
  Perfil de Gerenciamento:
  Changes Pending: No
```

O que Fazer Depois

Depois de criar o domínio do objeto, prossiga para a próxima etapa [“Etapa 3: configurando o armazenamento de objeto padrão”](#) na página 196.

Etapa 3: configurando o armazenamento de objeto padrão

Para configurar o armazenamento de objeto padrão para copiar dados do IBM Spectrum Protect Plus no Servidor IBM Spectrum Protect, efetue login no Operations Center e siga o procedimento para configurar conjuntos de armazenamentos. Conclua o processo seguindo as etapas para criar um serviço de agente de objeto usando o assistente do Operations Center.

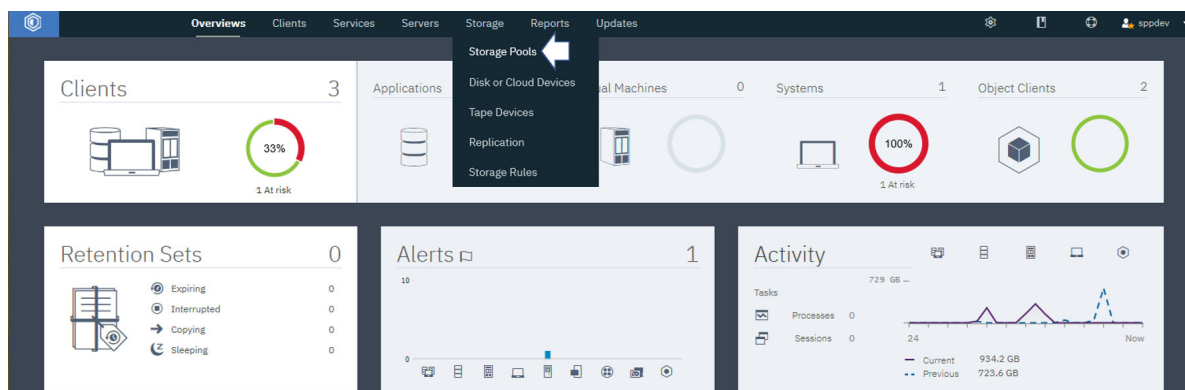
Antes de Iniciar

Antes de iniciar você deve configurar conjuntos de armazenamentos para armazenamento padrão ou para copiar na fita. Se estiver copiando na fita, você deverá configurar o conjunto de armazenamento em cache de dados frios, e para o armazenamento de objeto padrão, deve-se criar e configurar conjuntos de armazenamentos conforme necessário. Para obter instruções sobre como configurar o conjunto de armazenamento em cache de dados frios, consulte [“Etapa 1: criando um conjunto de armazenamento em fita e um conjunto de armazenamento em cache de dados frios para copiar dados para fita”](#) na página 193.

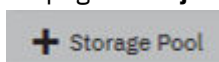
Procedimento

1. Crie um conjunto de armazenamentos de contêiner de diretório concluindo as seguintes etapas:

- a) Na barra de menus do Operations Center, clique em **Armazenamento** > **Conjuntos de armazenamentos**.



- b) Na página **Conjuntos de Armazenamentos**, clique em **Conjunto de Armazenamentos**



- c) Conclua as etapas no assistente para **Incluir conjunto de armazenamentos**.

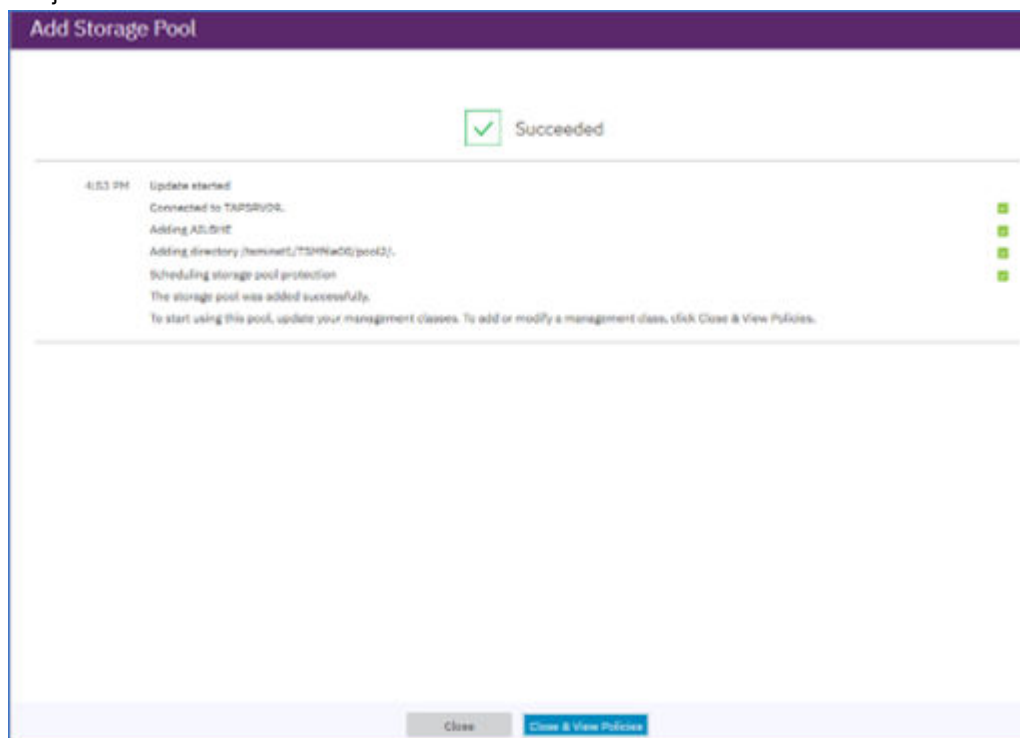
Dica: Selecione **Diretório** para o tipo de armazenamento baseado em contêiner e inclua diretórios com o ícone +. Clique em **Avançar** para continuar.

- d) Revise o resumo **Proteger Conjunto** e clique em **Avançar**.

- e) Especifique um conjunto de estouro necessário.

- f) Clique em **Incluir Conjunto de Armazenamentos** para concluir a criação do conjunto de armazenamentos.

Se a operação foi bem-sucedida, você verá um ícone para indicar o sucesso com um resumo do conjunto de armazenamentos.



2. Na página **Serviços** > **Políticas**, selecione uma política e clique em **Detalhes**.

Policy Domain	Server	Clients	Mgmt Classes	Option Sets	Schedules	Default Mgmt Class	Backup Destination	Archive Destination	Migration
IBM_DEPLOY_CLI...	P9B-AIX1	0	1	0	0	IBM_DEPLOY_CLIENT		DEDUPPOOL	
JASON	P9B-AIX1	0	2	0	0	STANDARD	DEDUPPOOL		
P9B-AIX1_DATABA...	P9B-AIX1	0	4	0	1	BACKUP_DISK_KEE...	DEDUPPOOL		
P9B-AIX1_DB2	P9B-AIX1	0	1	0	0	BACK_ARCH_DISK	DEDUPPOOL	DEDUPPOOL	

- É possível editar uma política de domínio existente seguindo estas etapas:
 - a) Atualize uma ou mais classes de gerenciamento para que use o novo conjunto editando o campo **Destino de backup** da tabela.
 - b) Clique em **Salvar**.
 - Ou, você pode criar um novo domínio executando o comando **definir objectdomain**. Para obter mais informações, consulte a etapa anterior “Etapa 2: configurando um domínio de política de objeto” na página 195.
3. Na página **Detalhes**, clique em **Seções de Política**. Clique no botão de alternância **Configurar** para tornar os conjuntos de políticas editáveis.

JASON P9B-AIX1


Active policy set: STANDARD Activated Apr 1, 2020, 8:25 PM

Default management class: STANDARD

Management Class	Default	Backup Destination
COLD		(None)
STANDARD	✓	DEDUPPOOL

Buttons: Cancel, Save

4. Altere o Destino de Backup para o conjunto de armazenamentos recém-criado, ou inclua uma nova

classe de gerenciamento,  **Management Class** para apontar para o novo conjunto de armazenamentos.

5. Clique em **Ativar**.
- A mudança do conjunto ativo de políticas pode resultar em perda de dados. Um resumo das diferenças entre o conjunto ativo de políticas e o novo conjunto de políticas é exibido antes de a mudança ser feita.
6. Revise as diferenças entre as classes de gerenciamento correspondentes nos dois conjuntos de políticas e considere as consequências nos arquivos do cliente. Arquivos do cliente que estão ligados às classes de gerenciamento no conjunto de políticas atualmente ativas são, após a ativação, ligados às classes de gerenciamento com os mesmos nomes no novo conjunto de políticas.
7. Identifique classes de gerenciamento no conjunto de políticas atualmente ativas que não têm contrapartes no novo conjunto de políticas e considere as consequências nos arquivos do cliente.

Arquivos do cliente que estão ligados a essas classes de gerenciamento são, após a ativação, gerenciados pela classe de gerenciamento padrão no novo conjunto de políticas.

8. Se as mudanças implementadas pelo conjunto de políticas forem aceitáveis, marque a caixa de seleção **Eu entendo que estas atualizações podem causar perda de dados** e clique em **Ativar**.

O que Fazer Depois

Crie e configure um cliente de objeto para o conjunto de armazenamentos ou conjuntos criados. Para obter informações adicionais, consulte [“Etapa 5: incluindo e configurando um cliente de objeto para copiar de dados”](#) na página 200

Etapa 4: incluindo um agente de objeto para copiar dados

Antes de poder copiar dados do IBM Spectrum Protect Plus no Servidor IBM Spectrum Protect, deve-se incluir e configurar o agente de objeto. Esta etapa é a quarta etapa na configuração do IBM Spectrum Protect Plus com o Servidor IBM Spectrum Protect para arquivar dados ou copiar dados para o armazenamento de objetos.

Antes de Iniciar

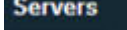
Assegure-se de que as etapas a seguir sejam concluídas antes de começar a criar o cliente de objeto.

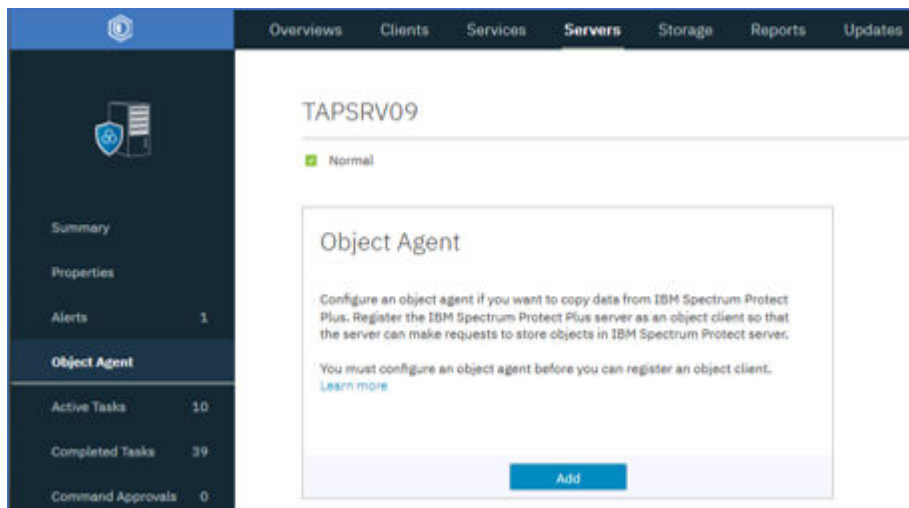
1. Assegure-se de que você tenha efetuado login no Servidor IBM Spectrum Protect com um ID do usuário da instância.
2. Assegure-se de ter configurado conjuntos de armazenamentos para armazenamento padrão ou para copiar em fita. Para obter instruções, consulte [“Etapa 1: criando um conjunto de armazenamento em fita e um conjunto de armazenamento em cache de dados frios para copiar dados para fita”](#) na página 193 ou [“Etapa 3: configurando o armazenamento de objeto padrão”](#) na página 196.
3. Certifique-se de que você criou um domínio de objetos.

Sobre Esta Tarefa

Este procedimento é baseado em um ambiente no qual o Servidor IBM Spectrum Protect é instalado em um sistema operacional IBM AIX AIX Versão 7.2 TL 1 e SP 4 ou mais recente, em execução em um servidor IBM POWER8 ou mais recente. (LINK PARA uma versão anterior)

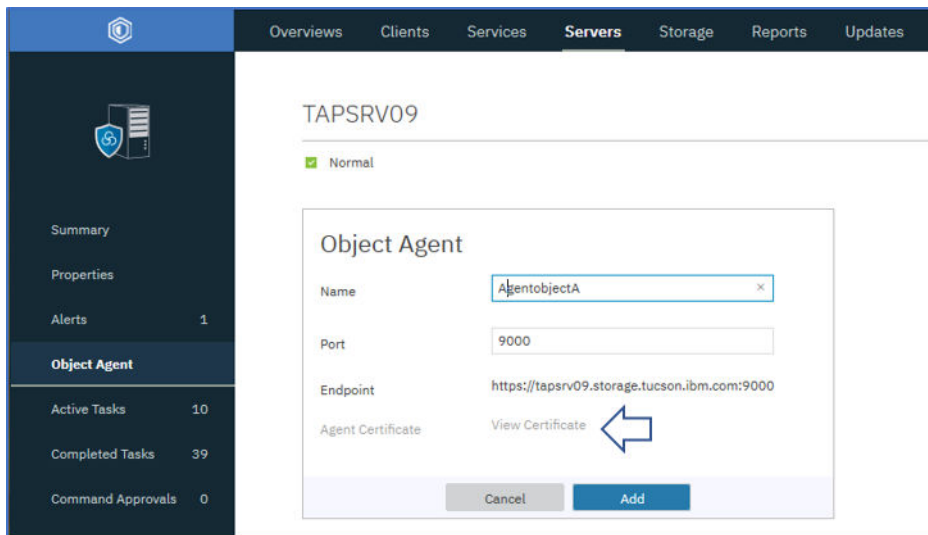
Procedimento

1. Na barra de menus do Operations Center, clique em **Servidores** .
2. Selecione um servidor e clique em **Detalhes**.
3. Na área de janela de navegação, clique em **Agente de Objeto**; clique em **Incluir** para incluir um agente de objeto.



Dica: Se você estiver usando a linha de comandos, execute o comando **DEFINE SERVER** para criar um agente de objeto. Especifique OBJECTAGENT=YES. Siga as instruções na saída de comando. Quando essas ações forem concluídas, o serviço de agente de objetos inicia automaticamente no sistema que está hospedando o Servidor IBM Spectrum Protect.

4. Para autenticar-se no agente de objeto, use o certificado que é gerado.



5. Instale o serviço do agente de objeto executando o comando que pode ser copiado do assistente, como nos exemplos a seguir:

```
[root@servername-os: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPP0BJAGENT/spObjectAgent_SPP0BJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Installed and started system service as
nameportnumberobjectagentname
```

Aqui está um exemplo

```
[root@p9b-aix1: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPP0BJAGENT/spObjectAgent_SPP0BJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Installed and started system service as spoa9000SPP0BJAGENT
```

6. Complete a configuração iniciando um serviço de agente de objetos executando o comando **startObjectAgent**. Aqui está um exemplo para o agente de objeto **AGENTOBJECTA**.

```
"/opt/tivoli/tsm/server/bin/spObjectAgent" service install
"/home/tsminst1/tsminst1/AGENTOBJECTA/spObjectAgent_AGENTOBJECTA_1500.config"
```

7. Configure o serviço do agente de objeto para iniciar automaticamente na inicialização executando um comando semelhante ao comando a seguir para o AIX:

```
spobj:2:once:/usr/bin/startsrc -s nameportnumberobjectagentname
```

A seguir encontra-se um exemplo:

```
spobj:2:once:/usr/bin/startsrc -s spoa9000SPP0BJAGENT
```

Etapa 5: incluindo e configurando um cliente de objeto para copiar de dados

Antes de poder copiar dados do IBM Spectrum Protect Plus no Servidor IBM Spectrum Protect, deve-se configurar o cliente do objeto. Essa etapa é a última etapa na configuração do Servidor IBM Spectrum Protect para arquivamento e cópia de dados com o Operations Center.

Antes de Iniciar

Assegure-se de que as etapas a seguir estejam concluídas antes de começar a criar o cliente de objeto.

1. Assegure-se de que você tenha efetuado login no Servidor IBM Spectrum Protect com um ID do usuário da instância.
2. Certifique-se de que os conjuntos de armazenamento para armazenamento padrão ou para cópia em fita estejam configurados e prontos. Para obter instruções, consulte [“Etapa 1: criando um conjunto de armazenamento em fita e um conjunto de armazenamento em cache de dados frios para copiar dados para fita”](#) na página 193 ou [“Etapa 3: configurando o armazenamento de objeto padrão”](#) na página 196.
3. Assegure-se de que um domínio de objeto e um agente de objeto sejam criados antes de iniciar.

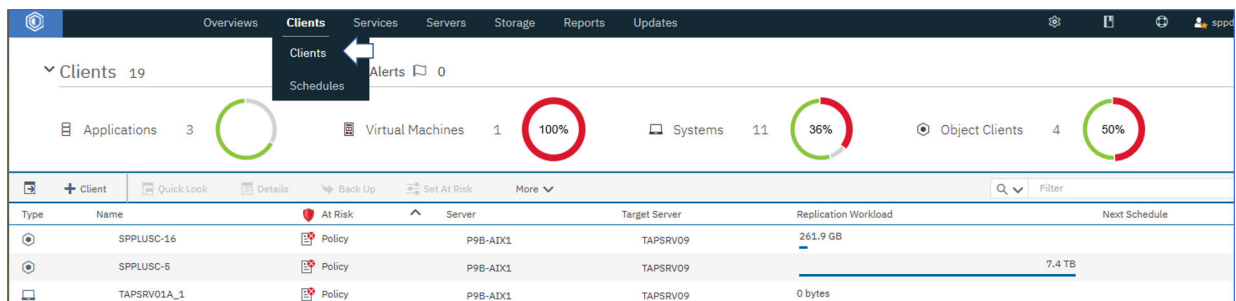
Dica: Se você criar um cliente de objeto antes de criar o agente de objeto correspondente, o assistente **Incluir Cliente** força a criação do agente de objeto.

Sobre Esta Tarefa

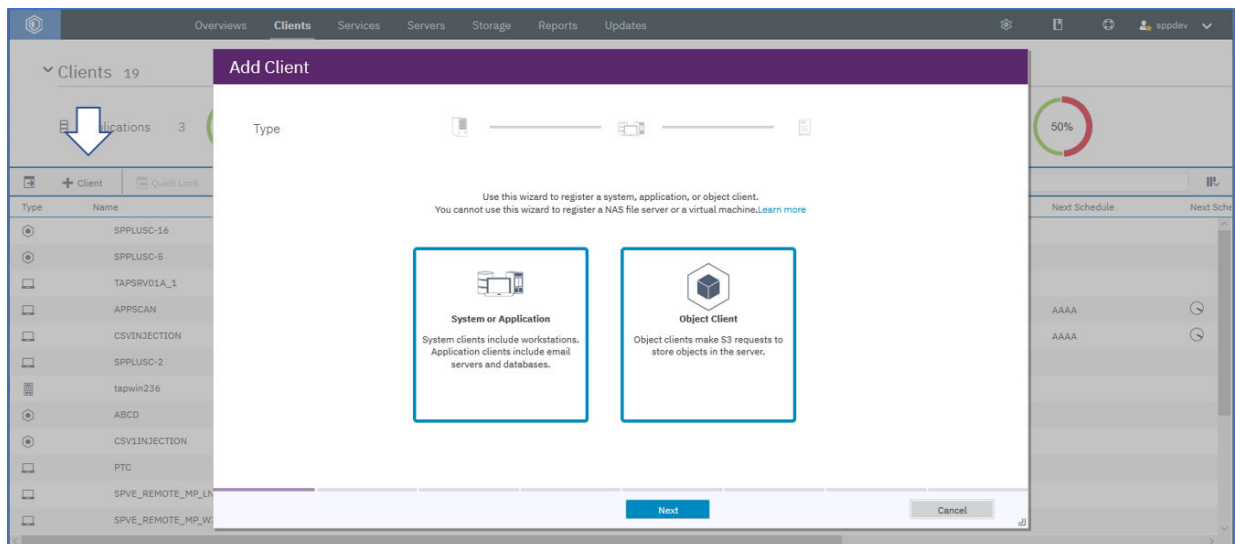
Este procedimento é baseado em um ambiente no qual o Servidor IBM Spectrum Protect é instalado em um sistema operacional IBM AIX Versão 7.2 TL 1 e SP 4 ou mais recente, em execução em um servidor IBM POWER8 ou mais recente.

Procedimento

1. Na barra de menus Operations Center, clique em **Clientes**.



2. Clique em **Cliente** para incluir um cliente conforme mostrado.



3. Selecione **Cliente do Objeto** e clique em **Avançar** para iniciar o assistente **Incluir Cliente**.

Nas telas do assistente, será solicitado que você faça as opções e definições a seguir para o cliente que está configurando.

- Você também pode optar por ativar a replicação para esse cliente.
- Você deve designar um nome de cliente e um nome de contato e um endereço de e-mail para relatório que você define na etapa final do assistente.

- Você deve designar um domínio de política, configurado na etapa 2, [“Etapa 2: configurando um domínio de política de objeto”](#) na página 195.
- É possível definir em relatório de risco para o cliente, como um relatório uma vez por dia para o endereço de e-mail que você especificou.

4. Clique em **Incluir Cliente**.

Nota:

Após a conclusão do processo, é fornecido um terminal para comunicação com o agente de objeto no servidor, o ID da chave de acesso, a chave de acesso secreta e o certificado para conexão de forma segura. Quando IBM Spectrum Protect Plus é um cliente de objeto, ele direciona os pedidos para o terminal e usa essas informações em forma de ID da chave de acesso, chave de acesso secreta e certificado seguro.

Importante: Assegure-se de que uma cópia de cada credencial seja salva em um local seguro.

Dica: Se você estiver usando a linha de comandos, execute o comando **REGISTER NODE** para criar um cliente de objeto. Especifique TYPE=OBJECTCLIENT. O script é executado sob o ID do usuário da instância.

O que Fazer Depois

Como uma próxima etapa, deve-se registrar o servidor IBM Spectrum Protect como um servidor de repositório. Para obter informações sobre como fazer isso, consulte [“Registrando um servidor de repositório como um provedor de armazenamento de backup”](#) na página 202. Uma vez concluída, é possível criar tarefas de política de SLA para copiar dados para o servidor IBM Spectrum Protect para armazenamento padrão ou para o archive para fita.

Registrando um servidor de repositório como um provedor de armazenamento de backup

Inclua e registre um servidor de repositório para ativar o IBM Spectrum Protect Plus para copiar 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 211 e [“Incluindo um Certificado”](#) na página 212.

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 transfere e armazena dados copiados. 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.

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 cópia são totalmente controladas por meio de políticas de SLA associadas em IBM Spectrum Protect Plus. As configurações de retenção do grupo de cópia do Servidor IBM Spectrum Protect não são usadas para operações de cópia.

Procedimento

Para incluir e registrar um Servidor IBM Spectrum Protect como um provedor de armazenamento de backup, conclua as etapas a seguir:

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 `qsevr 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 SLA que é usada para a tarefa de backup.	<p>Para criar uma política de SLA, consulte “Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos” na página 236.</p> <p>Para modificar uma política de SLA existente, consulte “Editando uma política de SLA” na página 247.</p>

Conceitos relacionados

[“Configuração para copiar ou arquivar dados para IBM Spectrum Protect”](#) na página 190


Se você estiver planejando copiar ou arquivar dados do IBM Spectrum Protect Plus para um Servidor IBM Spectrum Protect, há três configurações possíveis. A escolha de qual configurar depende de qual cenário se aplica às suas necessidades de proteção de dados. Para cada cenário, há etapas que são necessárias nos ambientes IBM Spectrum Protect Plus e Servidor IBM Spectrum Protect para concluir a configuração.

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 SLA 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 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, altere o rendimento para as operações de replicação e cópia do 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 20. 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, altere o rendimento para as operações de replicação e cópia do 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 21. 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.


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:

1. Na área de janela de navegação, clique em **Configuração do sistema > Site**.

2. Clique no ícone excluir  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 526](#)

Com o IBM Spectrum Protect Plus, é possível usar um servidor Lightweight Directory Access Protocol (LDAP) para gerenciar usuários. Ao criar uma conta do usuário LDAP, é possível incluir a conta do usuário em um grupo de usuários.

[“Planejando um relatório” na página 515](#)

É possível planejar relatórios em IBM Spectrum Protect Plus para serem executados 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 sAMAccountName 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 526](#)

Com o IBM Spectrum Protect Plus, é possível usar um servidor Lightweight Directory Access Protocol (LDAP) para gerenciar usuários. Ao criar uma conta do usuário LDAP, é possível incluir a conta do usuário em um grupo de usuários.

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 515](#)


É possível planejar relatórios em IBM Spectrum Protect Plus para serem executados 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.

Efetuando 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 SUPERUSER, insira o nome do usuário e a senha do 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.
System	Para efetuar logon como um usuário do sistema, insira a senha serveradmin. A senha padrão é sppDP758-SysXyz. É solicitado que mude esta senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em “Inicie o IBM Spectrum Protect Plus” na página 161 .

O que Fazer Depois

Revise a configuração do dispositivo virtual IBM Spectrum Protect Plus.

Conceitos relacionados

[“Requisitos de Sistema” na página 23](#)

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 521](#)

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.

Gerenciando Chaves e Certificados

Os recursos em nuvem e servidores de repositório requerem credenciais para servir como destinos de cópia. 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 do usuário e a senha dos seus destinos de cópia e permitem que eles sejam acessados pelo IBM Spectrum Protect Plus. Alguns destinos de cópias também requerem certificados para segurança de dados adicional.

Ao utilizar um recurso no IBM Spectrum Protect Plus que requer credenciais para acessar um destino de cópia, 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

É possível incluir uma chave SSH para fornecer credenciais para recursos baseados em Linux em máquinas virtuais gerenciadas pelo vCenter e Hyper-V, bem como servidores de aplicativos Oracle, Db2 e MongoDB. As chaves SSH ajudam a fornecer uma conexão segura entre IBM Spectrum Protect Plus e recursos de destino para operações de indexação de arquivos e restauração.

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.
- A conta do usuário no recurso de destino que é usado para gerar o par de chaves SSH deve ter privilégios **sudo**. Essa conta, que será designada ao IBM Spectrum Protect Plus, é conhecida como o agente do usuário do IBM Spectrum Protect Plus (sppagent).
- Se o ambiente incluir máquinas virtuais gerenciadas pelo vCenter, certifique-se de que as VMware Tools mais recentes estejam instaladas.

Procedimento

Para incluir uma chave, conclua as seguintes etapas:

1. No recurso de destino, gere uma chave SSH usando o comando `ssh-keygen` com a conta do usuário que será designada ao IBM Spectrum Protect Plus. Essa conta deve ter privilégios **sudo**. Por exemplo, em um servidor Oracle, insira o comando a seguir no terminal e siga as instruções:

```
ssh-keygen
```

Se você usar as configurações padrão, dois arquivos serão criados no diretório especificado: `id_rsa.pub` é a chave pública e `id_rsa` é a chave privada.

2. Quando solicitado, insira o nome do arquivo no qual a chave será salva, digite um nome de diretório e arquivo. Se você não especificar um diretório e nome de arquivo, o padrão será usado:

```
/home/privileged_user/.ssh/id_rsa
```

em que *privileged_user* é a conta designada ao IBM Spectrum Protect Plus, `sppagent`. Se uma chave com o nome padrão já existir, isso será indicado com a mensagem exibida abaixo. Tenha cuidado para não sobrescrever as chaves preexistentes se elas estiverem em uso. Pressione **N** para inserir um arquivo diferente no qual salvar a chave.

```
/home/<privileged user>/.ssh/id_rsa already exists.  
Sobrescrever (s/n)?
```

Esse procedimento baseia-se na suposição de que a chave é salva no local padrão usando o nome do arquivo padrão (`id_rsa`). Se o arquivo-chave for criado usando um nome de arquivo diferente, use esse nome de arquivo nas etapas que seguem.

3. Forneça uma passphrase e pressione Enter. Caso contrário, basta pressionar Enter para não fornecer nenhum passphrase.
4. Se um passphrase foi fornecido, digite-o novamente. Pressione Enter.
5. Copie o conteúdo da chave `id_rsa.pub` no arquivo `authorized_keys`. Se o arquivo já existir, anexe a chave pública ao arquivo `authorized_keys`.

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

6. Designe os privilégios necessários ao arquivo `authorized_keys` emitindo o comando `chmod 600`.

```
chmod 600 ~/.ssh/authorized_keys
```

7. Edite o arquivo `/etc/ssh/sshd_config` para definir a configuração `PubkeyAuthentication` como `yes` usando um editor de texto. Para assegurar que a configuração não seja comentada, remova o sinal de número (`#`) se ele aparecer no início da linha.

```
sudo vi /etc/ssh/sshd_config
```

```
...  
PubkeyAuthentication yes  
...
```

8. Reinicie o serviço SSH no recurso de destino.

```
systemctl restart sshd
```

9. Na área de janela de navegação do IBM Spectrum Protect Plus, clique em **Configuração do sistema** > **Chaves e certificados**.
10. Na seção **Chaves SSH**, clique em **Incluir chave SSH**.
11. Preencha os campos na área de janela **Propriedades da chave SSH**:

Nome

Insira um nome significativo para identificar a chave SSH.

Usuário

Insira a conta do usuário que está associada ao recurso de destino e chave SSH. Essa é a conta de usuário usada para gerar as chaves pública e privada nas etapas anteriores.

Criptografado

Marque esta caixa se um passphrase foi fornecido ao gerar as chaves pública e privada.

Passphrase

Esta caixa é exibida apenas se a caixa de seleção **Criptografado** for marcada. Se um passphrase foi fornecido ao gerar as chaves pública e privada, forneça o passphrase nesta caixa.

Chave Privada

Copie e cole a chave privada nesta caixa. Essa será a chave contida no arquivo `id_rsa` no recurso de destino. O arquivo é semelhante ao exemplo a seguir:

```
cat ~/.ssh/id_rsa
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
ZRYtuinjaHx2mKgW4LnFqzlyAIIq5Amasi/J8/AAAFiFiP4GZYj+BmAAAAB3NzaC1yc2
...
Q5ZqZ1Ec8N7dsAAAANDG9vckBVYnVudHVWQgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

12. Clique **Salvar**.


A chave é exibida na tabela **Chaves SSH** e pode ser selecionada quando você usa um recurso que requer credenciais para acessar um recurso com a 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.

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.

Antes de Iniciar

Assegure-se de que um certificado esteja disponível. As notas técnicas a seguir fornecem informações introdutórias para o uso de certificados com o IBM Spectrum Protect Plus:

HTTPS

Nota técnica [739663](#) fornece informações sobre o uso de um certificado HTTPS emitido pela Microsoft Certificate Authority. No entanto, é possível usar outra autoridade de certificação (CA).

LDAP

Nota técnica [791677](#) fornece informações sobre o uso de um certificado LDAP.

Para certificados HTTPS, os certificados codificados por PEM com extensões `.cer` ou `.crt` são suportados.

Para certificados LDAP, os certificados codificados pelo DER com extensões `.cer` ou `.crt` são suportados. Se você estiver carregando um certificado SSL do LDAP, assegure-se de que o IBM Spectrum Protect Plus possua 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.

Procedimento

Para fazer upload de um certificado SSL, conclua as seguintes etapas:

1. A partir de um navegador suportado, insira a URL a seguir para o console administrativo:

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

Em que *HOSTNAME* é o endereço IP da máquina virtual em que o console administrativo está implementado.

2. 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 SUPERUSER, insira o nome do usuário e a senha do administrador.
System	Para efetuar logon como um usuário do sistema, insira a senha serveradmin. A senha padrão é sppDP758-SysXyz. É solicitado que mude esta senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em “Inicie o IBM Spectrum Protect Plus” na página 161 .

3. Clique em **Gerenciamento de Certificados**.
4. Clique no tipo de certificado: **HTTP** ou **LDAP/Hyper-V**.
5. Clique em **Procurar** e selecione o certificado que você deseja transferir por upload.
6. Clique em **Fazer upload do certificado SSL para tipo de certificado**.
7. Quando o upload estiver concluído, clique em **Gerenciamento de Sistema > Reiniciar o IBM Spectrum Protect Plus**.

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 SUPERUSER, insira o nome do usuário e a senha do administrador.

Tipo de Autenticação	Informações de login
System	Para efetuar login como um usuário do sistema, insira a senha <code>serveradmin</code> . A senha padrão é <code>sppDP758-SysXyz</code> . É solicitado que mude esta senha durante o primeiro login. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em “Inicie o IBM Spectrum Protect Plus” na página 161 .

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. Reinicie o dispositivo IBM Spectrum Protect Plus a partir do Console Administrativo.
6. Uma vez que o dispositivo IBM Spectrum Protect Plus tenha sido reiniciado, visualize o fuso horário atual. Selecione **Informações do Produto** na página principal do Console Administrativo e verifique o fuso horário atualizado.

Efetuando login no dispositivo virtual

Efetue login 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 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 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-SysXyz`. É solicitado que mude esta senha durante o primeiro login. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).

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-SysXyz`. É solicitado que mude esta senha durante o primeiro logon. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).

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 por meio de uma 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 IBM Spectrum Protect Plus e um nó.

Procedimento

1. Faça login no dispositivo virtual IBM Spectrum Protect Plus usando o ID do usuário `serveradmin` e acesse a linha de comando. Execute o comando a seguir:

```
# sudo bash
```

2. Abra a porta 9000 no firewall executando o comando a seguir:

```
# firewall-cmd --add-port=9000/tcp
```

3. Execute a ferramenta executando o comando a seguir:

```
# 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 campos a seguir:

Host

O nome do host ou endereço IP do nó que você deseja testar.

Porta

A porta de conexão a ser testada.

6. Clique **Salvar**.
7. Para executar a ferramenta, passe o cursor sobre a ferramenta e, em seguida, clique em **Executar**. Se uma conexão não puder ser estabelecida, a condição de erro será exibida, junto com possíveis causas e ações.
8. Pare a ferramenta executando o comando a seguir na linha de comandos:

```
ctl-c
```

9. Proteja seu ambiente de armazenamento reconfigurando o firewall. Execute os seguintes comandos:

```
# 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 portas necessárias e reinicie o firewall com `iptables`. Para obter mais informações sobre a edição de regras de firewall, consulte a seção **Configuração do firewall com `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:

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 **pvdisk** 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-SysXyz`. É solicitado que mude esta senha durante o primeiro login. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).

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. A partir do console do dispositivo IBM Spectrum Protect Plus, emita os comandos a seguir:

```
sudo bash
```

Pressione Enter.

```
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-SysXyz`. É solicitado que mude esta senha durante o primeiro login. Determinadas regras são cumpridas ao criar uma nova senha. Para obter mais informações, consulte as regras de requisito de senha em [“Inicie o IBM Spectrum Protect Plus” na página 161](#).

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:

```
0 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 **pvcreeate /dev/sdd1**.

5. Para visualizar o novo PV a partir de /dev/sdd1, emita o comando **pvdiskdisplay**.
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
Sectores 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
```

Configurando preferências globais

Como administrador, você pode configurar preferências que se apliquem a todas as operações IBM Spectrum Protect Plus na área de janela **Preferências Globais**.

Antes de Iniciar

Você deve ter credenciais de administrador para configurar preferências globais.

É possível mudar a preferência na categoria **Integrações com outros produtos de armazenamento** a qualquer momento.



Atenção: Embora você possa modificar a preferência na categoria **Integrações com outros produtos de armazenamento**, modifique todas as outras preferências apenas se for absolutamente necessário e somente sob orientação do Suporte IBM. A modificação de preferências globais pode afetar seu ambiente de armazenamento. As preferências que requerem consulta do Suporte IBM estão nas seguintes categorias: **Aplicativo, Geral, Tarefa, Criação de Log, Proteção e Segurança**.

Sobre Esta Tarefa

Quaisquer mudanças que você fizer com os valores padrão de parâmetro se aplicam a todas as operações do IBM Spectrum Protect Plus quando você salva as mudanças.

Procedimento


Para editar os valores para qualquer configuração e aplicá-los globalmente, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Configuração do sistema > Preferências globais**.
2. Para permitir o acesso ao IBM Spectrum Protect Operations Center a partir de IBM Spectrum Protect Plus, edite a preferência na categoria **Integrações com outros produtos de armazenamento**. O valor padrão para a preferência é mostrado na figura a seguir:

É possível editar a preferência a seguir:

URL do Centro de Operações do IBM Spectrum Protect

O endereço IP do IBM Spectrum Protect Operations Center. O Operations Center fornece acesso à web e por dispositivo móvel a informações de status sobre o ambiente do IBM Spectrum Protect.

Quando essa preferência é configurada, o ícone do IBM Spectrum Protect  está ativo na barra de menus do IBM Spectrum Protect Plus. Ao configurar inicialmente a URL para essa preferência ou se você mudá-la, deve-se efetuar logoff e login novamente para que a preferência entre em vigor na interface com o usuário.

A URL é criada durante o processo de instalação do Operations Center. Para obter a URL do Operations Center, entre em contato com o administrador do sistema IBM Spectrum Protect.

3. Para aplicar as preferências de aplicativo global, edite as configurações na categoria **Aplicativo**. Os valores padrão para as preferências são mostrados na figura a seguir:

Application

Enable SQL Server databases restored in test mode eligible for backup

☐

Maximum volume size for backup target LUNs on Windows (TB)

Maximum backup retries(k8s)

Maximum concurrent servers running backups

Allow SQL database backup when transaction log backup chain is broken

☐

Rename SQL data and log files when database is restored in production mode with new name

☐

Você pode editar as seguintes preferências do aplicativo:

Ativar bancos de dados SQL Server restaurados no modo de teste elegíveis para backup

Fazer backup de bancos de dados SQL Server que foram restaurados no modo de teste. Quando essa opção é selecionada, os bancos de dados SQL Server que foram restaurados no modo de teste ficam disponíveis para seleção na área de janela Backup SQL ou no assistente de backup ad hoc.

Tamanho máximo do volume para os LUNs de destino de backup no Windows (TB)

O tamanho máximo do armazenamento para um destino de backup.

Máximo de novas tentativas de backup (k8s)

O número máximo de vezes que o IBM Spectrum Protect Plus tenta novamente as sessões de backup para uma tarefa de backup de cópia que contém várias solicitações de volume persistente (PVCs).

Quando vários PVCs estão envolvidos na mesma tarefa de backup de cópia, o IBM Spectrum Protect Plus executa as operações de backup como tarefas paralelas. Para ajudar a evitar que sessões de backup atinjam o tempo limite devido a problemas de conexão, especifique o número máximo de vezes que o IBM Spectrum Protect Plus tenta as conexões novamente.

Se o número máximo de novas tentativas for atingido e ainda houver falhas de conexão, apenas os backups da PVC que faziam parte das sessões com falha serão relatados como falhas.

Número máximo de servidores simultâneos que estão executando backups

O número máximo de servidores de aplicativos simultâneos por sessão de backup.

Permitir o backup do banco de dados SQL quando a cadeia de backup do log de transações for quebrada

Execute uma tarefa de backup de banco de dados quando o IBM Spectrum Protect Plus detectar uma quebra na cadeia de backup do log para um banco de dados.

Renomear arquivos de log e de dados SQL quando o banco de dados for restaurado no modo de produção com o novo nome

Renomeie arquivos de log e de dados do banco de dados SQL associado durante uma tarefa de restauração de produção ou de teste. Esse campo se aplica apenas quando um novo nome do banco de dados é fornecido durante uma tarefa de restauração do banco de dados SQL.

4. Para aplicar preferências gerais, edite as configurações na categoria **Geral**. Os valores padrão para as preferências são mostrados na figura a seguir:

General	
Access log retention (days)	<input type="text" value="30"/>
Tools working folder on Linux guest	<input type="text" value="/tmp"/>
Tools working folder on Windows guest	<input type="text" value="c:\\ProgramData"/>
Linux/AIX Clients Port (SSH) used for application and file indexing	<input type="text" value="22"/>
Windows Clients Port (WinRM) used for application and file indexing	<input type="text" value="5985"/>
IBM Spectrum Protect Plus Server IP Address	<input type="text"/>

Você pode editar as seguintes preferências gerais:

Retenção de log de acesso (dias)

Insira o número de dias que o log de acesso deve ser retido.

Pasta de trabalho de ferramentas no guest Linux

A pasta de trabalho para ferramentas em guests de VM Linux.

Pasta de trabalho de ferramentas no guest Windows

A pasta de trabalho para ferramentas em guests de VM Windows.

Porta dos Clientes Linux/AIX (SSH) usada para indexação de aplicativo e arquivo

A porta SSH que é usada para indexação de aplicativo e arquivo em clientes Linux e AIX.

A Porta dos Clientes Windows (WinRM) usada para indexação de aplicativo e arquivo

A Porta do Windows Remote Management (WinRM) que é usada para indexação de aplicativo e arquivo em clientes Windows.

Endereço IP do Servidor IBM Spectrum Protect Plus

A lista de endereços IP disponíveis para o servidor IBM Spectrum Protect Plus. Os endereços IP são usados para comunicação entre os proxies VADP e o servidor IBM Spectrum Protect Plus. Os endereços também são usados para comunicação de agente remoto.

5. Para aplicar as preferências de tarefa ou de criação de log, edite os valores nas categorias **Tarefa** ou **Criação de Log**. Os valores padrão para as preferências são mostrados na figura a seguir:

Job

Job log retention (days)

60

Job notification status

failed

Logging

Enable logging IBM Spectrum Protect Plus alerts to the system

☐

log

É possível editar as preferências de tarefa e de criação de log a seguir:

Retenção do log da tarefa (dias)

O número de dias para reter logs de tarefas antes de eles serem excluídos.

Status de notificação da tarefa

O nível de status para envio de alertas. Os alertas são enviados quando uma tarefa é concluída com o status especificado. Por exemplo, se o status de notificação de tarefa for **failed**, quando o status failed for relatado para uma tarefa, um alerta será enviado.

Ativar alertas do IBM Spectrum Protect Plus de criação de log para o log do sistema

Inclua alertas que são gerados pelo IBM Spectrum Protect Plus no log do sistema. Após você ativar esse recurso, será possível procurar o log do sistema para localizar alertas.

6. Para aplicar preferências de proteção, edite as configurações na categoria **Proteção**. Os valores padrão para as preferências são mostrados na figura a seguir:

Protection	
Number of seconds to wait before checking connection	1000
Number of times to check for valid connection	0
Temporary folder for file index zip files	/data2/filecatalog
Temporary folder for file indexing on Windows server	
Group VMs by	Count
Number of VMs in group	1
Force the removal of replication relationship for last remaining snapshot	<input type="checkbox"/>
Target free space error (percentage)	20
Target free space warning (percentage)	30
Catalog object update count	50
Virtual machine backup status update interval (seconds)	300
VADP proxy uses only HotAdd transport mode	<input type="checkbox"/>
VM group size (GB)	5120
vSnap auto disable deduplication when DDT size reaches resource limit	<input checked="" type="checkbox"/>
vSnap DDT size limit as percentage of total memory cache	80
vSnap DDT size limit in GB	50
Used space threshold on datastore or a volume before backup cannot take snapshots of a VM (percentage)	95
Backup wait timeout (seconds)	600
VMware communication timeout (seconds)	300

É possível editar as preferências de proteção a seguir:

Número de segundos a aguardar antes de verificar a conexão

A quantidade de tempo que o IBM Spectrum Protect Plus aguarda antes de verificar a conexão com um objeto de nuvem.

Número de vezes para verificar se há conexão válida

O número de vezes que o IBM Spectrum Protect Plus verifica uma conexão disponível.

Pasta temporária para arquivos zip de índice de arquivos

A pasta temporária para armazenar os arquivos compactados (.zip) que contêm os metadados para indexação. Quando a indexação é concluída, os arquivos são excluídos.

Pasta temporária para indexação de arquivo no servidor Windows

A pasta temporária para armazenar os arquivos compactados (.zip) que contêm os metadados para indexação do servidor Windows. Quando a indexação é concluída, a pasta é excluída.

Agrupar MVs por

As máquinas virtuais podem ser agrupadas. O grupo pode ser definido por uma contagem das VMs que estão incluídas no grupo ou pelo tamanho das VMs que estão incluídas no grupo.

Número de MVs no grupo

Para o agrupamento de VM, quatro grupos de VM estão disponíveis e cada grupo de VM pode ter um máximo de cinco VMs. Cada grupo corresponde a um volume de destino (fluxo de dados). No máximo 20 VMs (quatro fluxos de dados) pode ser agrupado de uma vez com base em cálculos de tamanho.

Forçar a remoção do relacionamento de replicação para a última captura instantânea restante

Remova um relacionamento de replicação existente para a última captura instantânea restante que está configurada para expirar e está bloqueada.

Erro de espaço livre de destino (porcentagem)

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.

Aviso de espaço livre de destino (porcentagem)

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.

Contagem de atualização de objeto do catálogo

A contagem que você pode configurar para limitar quantos objetos são consultados e atualizados no catálogo. Por exemplo, se o catálogo incluir 100 objetos e a contagem de atualizações for 20, o IBM Spectrum Protect Plus atualizará o catálogo em cinco iterações.

Intervalo de atualização do status de backup da máquina virtual (segundos)

A frequência em que as mensagens sobre o progresso da transferência de dados são atualizadas no log da tarefa.

Proxy VADP usa apenas o modo de transporte HotAdd

Use o método de transporte de disco virtual HotAdd para conectar o dispositivo virtual VMware IBM Spectrum Protect Plus com proxies VADP. Se essa opção estiver ativada, os proxies VADP usarão o HotAdd somente sem recuo para um modo de transporte alternativo.

Tamanho do grupo de VM (GB)

O tamanho, em gigabytes (GB), de grupos de VM.

vSnap desativa automaticamente a deduplicação quando o tamanho da DDT atinge o limite de recursos

A tabela de deduplicação (DDT) é ativada por padrão. Quando um dos limites definidos pelo espaço em disco (gigabytes) ou porcentagem é excedido, a deduplicação de dados vSnap é desativada e um alerta é exibido.

Limite de tamanho da DDT do vSnap como porcentagem do cache de memória total

O limite como uma porcentagem da tabela de deduplicação (DDT) do vSnap em comparação com o cache de memória total. A DDT será desativada quando a opção de desativação automática do vSnap for selecionada e o limite definido for excedido.

Limite de tamanho da DDT do vSnap em GB

O limite, em gigabytes (GB), da DDT do vSnap. A DDT será desativada quando a opção de desativação automática do vSnap for selecionada e o limite definido for excedido.

Limite de espaço usado no armazenamento de dados ou um volume antes do backup não pode fazer capturas instantâneas de uma VM (porcentagem)

A porcentagem de espaço usado em um armazenamento de dados ou um volume que é o limite antes das capturas instantâneas de uma VM não pode ser usada para backup.

Tempo limite de espera de backup (segundos)

A quantidade de tempo que o IBM Spectrum Protect Plus aguarda para uma tarefa de backup ser concluída antes de iniciar outra tarefa de backup. Se a tarefa de backup não for concluída dentro do período de espera, a tarefa atingirá o tempo limite e a próxima tarefa começará.

Tempo limite de conexão do VMware (segundos)

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.

7. Para aplicar uma preferência de segurança, edite a configuração na categoria **Segurança**. O valor padrão para a preferência é mostrado na figura a seguir:

Set Minimum Password Length (characters)

8

É possível editar a preferência de segurança a seguir:

Configurar Comprimento Mínimo de Senha (caracteres)

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.

Removendo o ambiente da Demo

O dispositivo IBM Spectrum Protect Plus inclui um servidor vSnap integrado denominado host local, um site para propósitos de demonstração que é denominado Demo e uma política de SLA associada que é denominada Demo. Para ambientes de produção maiores, não use o servidor vSnap integrado. Em vez disso, use um ou mais servidores vSnap independentes. A política de SLA Demo, o site Demo e o servidor vSnap integrado, coletivamente o ambiente Demo, podem ser removidos com segurança para conservar o espaço em disco.

Antes de Iniciar

Para os dispositivos do IBM Spectrum Protect Plus que estão em produção, faça backup do aplicativo IBM Spectrum Protect Plus. Para obter instruções, consulte [“Fazendo backup do aplicativo IBM Spectrum Protect Plus”](#) na página 491. Para novas implementações, não é necessário fazer o backup do aplicativo.

Verifique se os dados no servidor vSnap do host local não são necessários.


Assegure-se de que pelo menos um servidor vSnap independente seja implementado como um destino de backup.





Sobre Esta Tarefa


Quando implementado, um dispositivo IBM Spectrum Protect Plus possui seis discos rígidos virtuais. Ao remover a configuração Demo e o servidor vSnap do host local do dispositivo IBM Spectrum Protect Plus, é possível liberar o armazenamento através da remoção de dois dos discos rígidos virtuais associados.

O procedimento neste tópico deve ser seguido a fim de remover o ambiente Demo de IBM Spectrum Protect Plus.

Procedimento


1. Desative as políticas de SLA que são designadas ao ambiente Demo concluindo as seguintes etapas:
 - a) A partir de um navegador suportado, efetue login na interface com o usuário do IBM Spectrum Protect Plus.
 - b) Visualize todas as tarefas que são designadas ao SLA Demo. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**. Localize qualquer tarefa que siga o padrão de nomenclatura *Job_Name_Demo*, em que *Job_Name* é o nome da tarefa. Esse padrão de nomenclatura indica que o SLA Demo é usado.
 - c) Pause o planejamento para cada tarefa Demo. Clique no ícone do menu de ações  e selecione **Pausar Planejamento** para cada tarefa que termina em *_Demo*.
2. Exclua o SLA Demo concluindo as etapas a seguir:
 - a) Na área de janela de navegação, clique em **Gerenciar Proteção > Visão Geral da Política**. Role para baixo na tabela na área de janela Políticas de SLA e localize a política Demo.

- b) Clique no ícone excluir  ao lado do SLA Demo.
 - c) Insira o código na caixa de diálogo **Confirmar** e clique em **OK**.
 3. Exclua o armazenamento de disco vSnap do host local concluindo as etapas a seguir:
 - a) Na área de janela de navegação, clique em **Configuração do Sistema > Armazenamento de Backup > Disco**. Localize o armazenamento vSnap do host local designado ao site Demo.
 - b) Clique no ícone excluir  ao lado do armazenamento vSnap do host local.
 - c) Insira o código na caixa de diálogo **Confirmar** e clique em **DELETE**.
 4. Exclua o site Demo concluindo as etapas a seguir:
 - a) Na área de janela de navegação, clique em **Configuração do Sistema > Site**. Localize o site denominado Demo.
 - b) Clique no ícone excluir  ao lado do site Demo.
 - c) Clique em **Sim** na caixa de diálogo **Confirmar** para concluir a remoção do site Demo.
 5. Remova a identidade LocalvSnapAdmin concluindo as etapas a seguir:
 - a) No painel de navegação, clique em **Contas > Identidade**.
 - b) Clique no ícone excluir  ao lado da identidade LocalvSnapAdmin.
 - c) Clique em **Sim** na caixa de diálogo **Confirmar** para remover a identidade.
 6. Limpe as configurações do sistema de arquivos e LVM concluindo as etapas a seguir:
 - a) Efetue login no IBM Spectrum Protect Plus usando o protocolo do Secure Shell (SSH) ou através do console do hypervisor usando a conta `serveradmin`.
 - b) Obtenha o ID do conjunto de armazenamento vSnap do host local. Emita o seguinte comando:

```
$ vsnap pool show
```
 -  **Atenção:** Para garantir que nenhum dado seja perdido, verifique se o ID obtido é o ID do conjunto de armazenamento vSnap do host local.
 - c) Exclua o conjunto de armazenamento vSnap do host local. Emita o comando a seguir em que *<ID>* é o ID obtido na etapa anterior:

```
$ vsnap pool delete --id <ID>
```
 - d) Desmonte o cache de nuvem de armazenamento vSnap do host local. Emita o seguinte comando:

```
$ sudo umount -f /opt/vsnap-data
```
 - e) Edite o arquivo `fstab` para desativar o cache de nuvem desde o início. Usando `sudo` e um editor de texto, comente a linha iniciando com `/dev/mapper/vsnapdata-vsnapdata1v`.
 - f) Desative o grupo de volumes LVM que está associado ao cache de nuvem. Emita o seguinte comando:

```
$ sudo vgchange -an vsnapdata
```
 7. Usando o vSphere ou o Hyper-V Manager, desconecte os discos rígidos virtuais que não são mais necessários do dispositivo IBM Spectrum Protect Plus. prossiga com cautela para assegurar que os discos corretos sejam desconectados. O servidor vSnap do host local possui dois discos rígidos virtuais associados, que têm 100 GB e 128 GB de tamanho. Para instruções detalhadas sobre a desconexão ou remoção de discos rígidos virtuais, consulte a documentação do hypervisor apropriado. Um procedimento geral para cada hypervisor é apresentado a seguir.
 **Atenção:** Desligue o dispositivo IBM Spectrum Protect Plus antes de desconectar os discos rígidos virtuais. Não exclua os discos rígidos virtuais até que a funcionalidade adequada tenha sido confirmada após ligar o dispositivo e a execução da tarefa de manutenção.
- Remova os discos rígidos virtuais associados da máquina virtual concluindo as etapas a seguir:

- a) Para ambientes VMware, abra o vSphere e conclua as etapas a seguir:
- 1) Clique em **VMs e Modelos**.
 - 2) Expanda o host que contém o dispositivo IBM Spectrum Protect Plus.
 - 3) Selecione a máquina virtual IBM Spectrum Protect Plus.
 - 4) Desligue o dispositivo do IBM Spectrum Protect Plus.
 - 5) A partir do menu **Ações**, clique em **Editar Configurações**.
 - 6) Localize os discos rígidos virtuais que não são mais necessários. Os tamanhos ao lado dos discos que podem ser removidos são 100 GB e 128 GB.
 - 7) Selecione um dos discos identificados e clique no botão Remover.
Importante: Não marque a caixa de seleção **Excluir Arquivos do Armazenamento de Dados** para o disco. Exclua os discos somente após a verificação da funcionalidade adequada.
 - 8) Selecione o disco identificado restante e clique no botão Remover.
 - 9) Clique em **OK**.
 - 10) Ligue o IBM Spectrum Protect Plus.
- b) Para ambientes Hyper-V, abra o Hyper-V Manager e conclua as etapas a seguir:
- 1) Selecione o nó ao qual a máquina virtual IBM Spectrum Protect Plus pertence.
 - 2) Selecione a máquina virtual IBM Spectrum Protect Plus a partir da área de janela **Máquinas Virtuais**.
 - 3) Desligue o dispositivo do IBM Spectrum Protect Plus.
 - 4) Clique em **Configurações** da máquina virtual.
 - 5) Localize os discos rígidos virtuais que não são mais necessários. Para cada disco rígido virtual conectado, clique em Inspeccionar. Os valores **Tamanho Máximo do Disco** na janela **Propriedades do Disco Rígido Virtual** devem ser 100 GB e 128 GB.
 - 6) Selecione um dos discos identificados e clique em **Remover**.
 - 7) Selecione o disco identificado restante e clique em **Remover**.
 - 8) Clique em **OK**.
 - 9) Ligue o IBM Spectrum Protect Plus.
8. Varra novamente o barramento SCSI e desative o serviço vSnap concluindo as etapas a seguir:
- a) Efetue login no IBM Spectrum Protect Plus usando o protocolo do Secure Shell (SSH) ou através do console do hypervisor usando a conta serveradmin.
 - b) Varra novamente o barramento SCSI emitindo o seguinte comando:

```
$ sudo rescan-scsi-bus.sh
```
 - c) Pare o serviço vSnap emitindo o comando a seguir:

```
$ sudo systemctl stop vsnap
```
 - d) Desative o serviço vSnap emitindo o seguinte comando:

```
$ sudo systemctl disable vsnap
```

Capítulo 9. Gerenciando 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 de replicar ou copiar 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. Para todos os recursos suportados, exceto para instâncias e contêineres do Amazon EC2.

Prata

Esta política é executada diariamente com um período de retenção de 1 mês. Para todos os recursos suportados, exceto para as instâncias do Amazon EC2 e dados do contêiner.

Bronze

Esta política é executada diariamente com um período de retenção de 1 semana. Para todos os recursos suportados, exceto para as instâncias do Amazon EC2 e dados do contêiner.

EC2

Para proteger as instâncias do Amazon EC2, essa política executa backups de captura instantânea diária com um período de retenção de 31 dias.

Contêiner

Para proteger os dados do contêiner, esta política executa as operações a seguir:

- Backups de captura instantânea a cada seis horas com um período de retenção de um dia
- Backups de cópia diários com um período de retenção de 31 dias.

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 SLA existente alterando as opções de origem da cópia de armazenamento de objeto padrão, tipo de destino ou servidor 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 Plus, uma configuração demo de SLA está disponível para testes. 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 de 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.

Resumo de Proteção

É possível visualizar o status de proteção dos recursos em seu sistema na área de janela **Resumo de Proteção**.

A área de janela **Resumo de Proteção** consiste em gráficos de rosca que retratam o número de recursos protegidos versus o número de recursos desprotegidos. Para cada tipo de recurso, é possível visualizar a porcentagem do recurso que está protegida e a política de acordo de nível de serviço (SLA) que é usada com mais frequência para esse recurso.

Para visualizar a área de janela **Resumo de Proteção**, a partir da área de janela de navegação, clique em **Gerenciar Proteção > Visão Geral de Política**.

Policy Overview



System

O gráfico **Seu Sistema** mostra a porcentagem total de recursos em seu sistema que são protegidos por IBM Spectrum Protect Plus.

% protegida

Mostra a porcentagem de recursos que são protegidos por IBM Spectrum Protect Plus. No gráfico de rosca, os recursos protegidos são representados pela linha azul. Ao passar o mouse sobre as diferentes partes da rosca, é possível visualizar os números de recursos protegidos e desprotegidos.

Recursos desprotegidos

Mostra a legenda de recursos desprotegidos. Na lista, os dados são mostrados apenas para os tipos de recursos que são gerenciados por sua instância do IBM Spectrum Protect Plus. Se um tipo de recurso não for gerenciado por IBM Spectrum Protect Plus, a contagem será 0.

Sistemas virtualizados

O gráfico **Sistemas Virtualizados** mostra a porcentagem de sistemas virtualizados que são protegidos por IBM Spectrum Protect Plus.

% protegida

Mostra a porcentagem de sistemas virtualizados que são protegidos. Ao passar o mouse sobre as diferentes partes da rosca, é possível visualizar os números de sistemas virtualizados protegidos e desprotegidos.

Se nenhum sistema virtualizado for gerenciado por IBM Spectrum Protect Plus, a porcentagem será 0.

Política mais usada

Mostra o nome da política de SLA usada com mais frequência e o número de sistemas virtualizados que estão usando essa política. Se nenhum sistema virtualizado for gerenciado por IBM Spectrum Protect Plus, esse campo não será exibido.

Nenhuma política protegida

Esta mensagem é mostrada apenas quando nenhum sistema virtualizado é gerenciado por IBM Spectrum Protect Plus.

Bancos de dados

O gráfico **Bancos de Dados** mostra a porcentagem de bancos de dados que são protegidos por IBM Spectrum Protect Plus.

% protegida

Mostra a porcentagem de bancos de dados que são protegidos. Ao passar o mouse sobre as diferentes partes da rosca, é possível visualizar os números de bancos de dados protegidos e desprotegidos.

Se nenhum banco de dados do aplicativo for gerenciado por IBM Spectrum Protect Plus, a porcentagem será 0.

Política mais usada

Mostra o nome da política de SLA usada com mais frequência e o número de bancos de dados que estão usando essa política. Se nenhum banco de dados for gerenciado por IBM Spectrum Protect Plus, este campo não será exibido.

Nenhuma política protegida

Esta mensagem é mostrada apenas quando nenhum banco de dados é gerenciado por IBM Spectrum Protect Plus.

Nuvem

O gráfico **Nuvem** mostra a porcentagem de contas baseadas em nuvem, como os locatários do Microsoft Office 365, que são protegidos por IBM Spectrum Protect Plus.

% protegida

Mostra a porcentagem de contas baseadas em nuvem que estão protegidas. Ao passar o mouse sobre as diferentes partes da rosca, é possível visualizar os números de contas protegidas e desprotegidas.

Se nenhuma conta baseada em nuvem for gerenciada por IBM Spectrum Protect Plus, a porcentagem será 0.

Política mais usada

Mostra o nome da política de SLA usada com mais frequência e o número de contas que estão usando essa política. Se nenhuma conta baseada em nuvem for gerenciada por IBM Spectrum Protect Plus, este campo não será exibido.

Nenhuma política protegida

Esta mensagem é mostrada apenas quando nenhuma conta baseada em nuvem é gerenciada por IBM Spectrum Protect Plus.

Volumes persistentes de contêineres

Mostra a porcentagem de volumes persistentes que são protegidos por IBM Spectrum Protect Plus.

% protegida

Mostra a porcentagem de volumes persistentes que são protegidos. Ao passar o mouse sobre as diferentes partes da rosca, é possível visualizar os números de volumes protegidos e desprotegidos.

Se nenhum volume persistente for gerenciado por IBM Spectrum Protect Plus, a porcentagem será 0.

Política mais usada

Mostra o nome da política de SLA usada com mais frequência e o número de volumes persistentes que estão usando essa política. Se nenhum volume persistente for gerenciado por IBM Spectrum Protect Plus, este campo não será exibido.

Nenhuma política protegida

Esta mensagem é mostrada apenas quando nenhum volume persistente é gerenciado por IBM Spectrum Protect Plus.

Sistemas de Arquivos

Mostra a porcentagem de sistemas de arquivos que são protegidos por IBM Spectrum Protect Plus.

% protegida

Mostra a porcentagem de sistemas de arquivos que estão protegidos. Ao passar o mouse sobre as diferentes partes da rosca, é possível visualizar os números de sistemas de arquivos protegidos e desprotegidos.

Se nenhum sistema de arquivos for gerenciado por IBM Spectrum Protect Plus, a porcentagem será 0.

Política mais usada

Mostra o nome da política de SLA usada mais frequentemente e o número de sistemas de arquivos que estão usando essa política. Se nenhum sistema de arquivos for gerenciado por IBM Spectrum Protect Plus, este campo não será exibido.

Nenhuma política protegida

Esta mensagem é mostrada apenas quando nenhum sistema de arquivos é gerenciado por IBM Spectrum Protect Plus.

Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos

Você pode criar políticas de acordo de nível de serviço (SLA) customizadas para definir as políticas de frequência de backup, retenção, replicação e cópia que são específicas para o seu ambiente.

Sobre Esta Tarefa

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

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 SLA.

Ao copiar dados de um servidor vSnap para o armazenamento em nuvem, a captura instantânea concluída com sucesso mais recente será copiada.

Procedimento

Para criar uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos, complete 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 SLA** é exibida.
3. No campo **Nome**, insira um nome que forneça uma descrição significativa da política de SLA.

4. Clique em **Sistemas de arquivos VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB e Windows**.
5. Na seção **Política de backup**, configure as opções a seguir 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 que são criadas sem um planejamento podem ser executadas on demand.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de backup. Escolha entre **Minutos**, **Horas**, **Dias**, **Semanas**, **Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

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

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

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.

6. 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 [“Configurando parceiros de armazenamento de backup” na página 120](#).

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

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de replicação. Escolha entre **Minutos, Horas, Dias, Semanas, Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

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

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

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.

7. Na seção **Cópias Adicionais**, configure as opções a seguir para copiar dados para o armazenamento de objeto padrão ou armazenamento de objeto de archive.

Armazenamento de objeto padrão (cópia incremental)

Selecione esta opção para copiar dados para o armazenamento em nuvem ou para um servidor do repositório.

Os dados são submetidos a backup para o servidor vSnap para proteção de curto prazo e, em seguida, copiados para o servidor de armazenamento em nuvem ou repositório selecionado para proteção de longo prazo. Durante a primeira cópia de um volume de backup, é feito backup completo da captura instantânea. Depois que a primeira cópia da captura instantânea de base for concluída, as cópias subsequentes serão incrementais e capturarão mudanças acumulativas desde a última cópia. As operações de restauração do servidor em nuvem ou de repositório podem ser executadas a partir de qualquer servidor vSnap disponível.

Desativar Programação

Marque esta caixa de seleção para criar o relacionamento de cópia sem definir uma frequência ou horário de início.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de cópia. Escolha entre **Minutos, Horas, Dias, Semanas, Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

Insira a data e hora na qual deseja que a operação de cópia seja iniciada.

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por

exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

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.

Restrição: As opções de retenção de cópias serão desativadas se um servidor que usa retenção Write Once Read Many (WORM) for selecionado no campo **Destino**.

Origem

Clique na origem para a operação de cópia:

Destino da Política Principal

A origem para a operação de cópia é o site de destino que está definido na seção **Política Principal**.

Destino da Política de Replicação

A origem para a operação de cópia é o site de destino que é definido na seção **Política de replicação**.

Essa opção estará disponível somente quando **Replicação de armazenamento de backup** for selecionada.

Destination

Clique em **Serviços de nuvem** ou **Servidores do repositório**.

Resposta

Clique no sistema de armazenamento em nuvem ou no servidor do repositório para o qual você deseja copiar 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 183 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.

Armazenamento de objeto de archive (cópia completa)

Selecione essa opção para arquivar dados no armazenamento em nuvem ou em um servidor do repositório para proteção de longo prazo.

Esta operação fornece uma cópia de imagem completa para o armazenamento de arquivo selecionado.

Desativar Programação

Marque essa caixa de seleção para criar o relacionamento de archive sem definir uma frequência ou um horário de início.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de archive. Escolha entre **Minutos**, **Horas**, **Dias**, **Semanas**, **Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

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

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

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 **Serviços de nuvem** ou **Servidores do 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 183](#).

8. Clique em **Save**. A política de SLA agora pode ser aplicada a definições de tarefa de backup.

O que Fazer Depois

Depois de criar uma política de SLA, conclua as seguintes ações:

Ação	Como
Designar permissões de usuário à política de SLA.	Consulte “Criando uma função” na página 523
Crie uma definição de tarefa de backup que use a política de SLA.	Consulte os tópicos de backup em Capítulo 10, “Protegendo sistemas virtualizados”, na página 249, Capítulo 14, “Protegendo bancos de dados”, na página 363 e Capítulo 11, “Protegendo sistemas de arquivos”, na página 299.

Conceitos relacionados

[“Replicar dados de armazenamento de backup” na página 11](#)

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.

[“Copiar capturas instantâneas para armazenamento de backup secundário” na página 11](#)

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 copiar capturas instantâneas de um servidor vSnap para o armazenamento de backup secundário.

Tarefas relacionadas

[“Criando uma política de SLA para instâncias do Amazon EC2” na página 241](#)

É possível criar políticas de acordo de nível de serviço customizado (SLA) para definir políticas de retenção e frequência de captura instantânea que são específicas para instâncias do Amazon EC2.

[“Criando uma política de SLA para cluster de Kubernetes” na página 242](#)

É possível criar políticas de acordo de nível de serviço (SLA) customizadas para volumes persistentes que estão conectados a um cluster de Kubernetes. É possível definir a frequência de operações de captura instantânea e de backup e especificar políticas para tarefas de retenção, replicação e cópia.

Criando uma política de SLA para instâncias do Amazon EC2

É possível criar políticas de acordo de nível de serviço customizado (SLA) para definir políticas de retenção e frequência de captura instantânea que são específicas para instâncias do Amazon EC2.

Sobre Esta Tarefa

Quando uma tarefa de backup planejada é executada, uma captura instantânea da instância é criada na frequência que é definida pela política de captura instantânea.

Se uma instância estiver associada a várias políticas de SLA, assegure-se de que as políticas criadas não estejam planejadas para serem executadas simultaneamente. Planeje as políticas de SLA para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de SLA.

Procedimento

Para criar uma política de SLA para suas instâncias, 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 SLA** é exibida.

3. No campo **Nome**, insira um nome que forneça uma descrição significativa da política de SLA.
4. Clique em **Amazon EC2**.

As opções de política de SLA para instâncias EC2 são exibidas.

5. Na seção **Proteção de captura instantânea**, configure as opções a seguir para operações de captura instantânea:

Retenção

Especifique o período de retenção para as capturas instantâneas.

Desativar Programação

Marque esta caixa de seleção para criar a política de captura instantânea sem definir uma frequência ou horário de início. As políticas que são criadas sem um planejamento podem ser executadas sob demanda. Este campo é opcional.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de captura instantânea. Escolha entre **Minutos**, **Horas**, **Dias**, **Semanas**, **Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

Insira a data e hora na qual deseja que a operação de captura instantânea seja iniciada.

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

Prefixo de captura instantânea

Insira um prefixo para incluir no início dos nomes de captura instantânea. Os prefixos podem ajudá-lo a organizar e a identificar facilmente capturas instantâneas. Este campo é opcional.

Por exemplo, se você inseriu o prefixo "daily_", todos os nomes de capturas instantâneas que forem criados com esta política de SLA começarão com "daily_".

6. Clique em **Salvar**.

A política de SLA que você criou é exibida na tabela na área de janela de Políticas de SLA.

O que Fazer Depois

Depois de criar uma política de SLA, conclua as seguintes ações:

- Designe permissões de usuário à política de SLA. Para obter instruções, consulte [“Criando uma função”](#) na página 523.
- Crie uma definição de tarefa de backup que use a política de SLA. Para obter instruções, consulte [“Fazendo backup de dados do Amazon EC2”](#) na página 291.

Tarefas relacionadas

[“Editando uma política de SLA”](#) na página 247

Edite as opções para uma política de SLA para refletir mudanças no ambiente IBM Spectrum Protect Plus.

[“Excluindo uma política de SLA”](#) na página 247

Exclua uma política de SLA quando ela se tornar obsoleta.

Criando uma política de SLA para cluster de Kubernetes

É possível criar políticas de acordo de nível de serviço (SLA) customizadas para volumes persistentes que estão conectados a um cluster de Kubernetes. É possível definir a frequência de operações de captura instantânea e de backup e especificar políticas para tarefas de retenção, replicação e cópia.

Antes de Iniciar

Se você planeja copiar dados para o armazenamento secundário ou arquivar dados para um sistema de armazenamento em nuvem, execute as ações a seguir:

- Se você planeja copiar dados para o armazenamento secundário, como um sistema de armazenamento em nuvem ou servidor de repositório, assegure-se de que o armazenamento secundário esteja configurado. Para obter informações sobre os sistemas de armazenamento secundário que são suportados e instruções de configuração, consulte [“Gerenciando o armazenamento de backup secundário”](#) na página 183
- Se você planeja arquivar dados para um sistema de armazenamento em nuvem, o destino da nuvem deverá ter um depósito de archive definido. Para incluir um depósito de archive para um sistema de armazenamento em nuvem, siga as instruções em [“Gerenciando o armazenamento em”](#) na página 183.

Sobre Esta Tarefa

É possível criar políticas de SLA customizadas se você não quiser usar a política de **Contêiner** predefinida. A política **Contêiner** executa as operações a seguir:

- Fazer backups de captura instantânea a cada seis horas com um período de retenção de um dia
- Copiar backups diariamente com um período de retenção de 31 dias

Uma captura instantânea é necessária em uma operação de backup do Kubernetes. Quando uma tarefa de backup planejada é executada, uma captura instantânea da solicitação de volume persistente (PVC) é criada no sistema de armazenamento Ceph na frequência que é definida pela política de captura instantânea. É possível especificar configurações de políticas adicionais para copiar a captura instantânea para o servidor vSnap IBM Spectrum Protect Plus, replicar o servidor vSnap ou copiar os dados para o armazenamento de objeto na nuvem ou em um servidor de repositório.

Se uma PVC estiver associada a várias políticas de SLA, assegure-se de que as políticas criadas não estejam planejadas para serem executadas simultaneamente. Planeje as políticas de SLA para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de SLA.

Procedimento

Para criar uma política de SLA para suas PVCs, conclua as etapas a seguir:

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 SLA** é exibida.

3. No campo **Nome**, insira um nome que forneça uma descrição significativa da política de SLA.
4. Clique em **Kubernetes**.
As opções de política de SLA para clusters Kubernetes são exibidas.
5. Na seção **Proteção de captura instantânea**, configure as opções a seguir para as operações de captura instantânea.

Retenção

Especifique o período de retenção para as capturas instantâneas.

Desativar Programação

Marque esta caixa de seleção para criar a política de captura instantânea sem definir uma frequência ou horário de início. As políticas que são criadas sem um planejamento podem ser executadas sob demanda. Este campo é opcional.

Se você planeja ativar as seções de política para operações de backup de cópia, replicação ou de cópias adicionais, assegure-se de que esta caixa de seleção não esteja marcada. Caso contrário, nenhuma captura instantânea estará disponível para cópia no servidor do vSnap.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de captura instantânea. Escolha entre **Minutos**, **Horas**, **Dias**, **Semanas**, **Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

Insira a data e hora na qual deseja que a operação de captura instantânea seja iniciada.

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

Prefixo de captura instantânea

Insira um prefixo para incluir no início dos nomes de captura instantânea. É possível incluir um prefixo em nomes de capturas instantâneas para ajudá-lo a organizar e identificar facilmente capturas instantâneas. Este campo é opcional.

É possível inserir até 32 caracteres para o prefixo.

Por exemplo, se você inseriu o prefixo "daily", todos os nomes de capturas instantâneas que forem criados com esta política de SLA começarão com "daily".

6. Opcional: Na seção **Política de Backup**, configure as opções a seguir para operações de backup de cópia para o servidor vSnap:

Armazenamento de Backup

Marque esta caixa de seleção para ativar as operações de backup de cópia para o servidor vSnap. 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 os backups de cópia no servidor vSnap.

Desativar Programação

Marque esta caixa de seleção para criar a política de backup sem definir uma frequência ou horário de início. As políticas que são criadas sem um planejamento podem ser executadas sob demanda. Este campo é opcional.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de backup de cópia. Escolha entre **Minutos, Horas, Dias, Semanas, Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

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

Dica: Distribua o tempo para o backup de captura instantânea ser concluído antes do início da operação de backup de cópia. Por exemplo, se a operação de captura instantânea iniciar à meia-noite (0:00), configure a operação de backup de cópia para iniciar 15 minutos depois, às 00:15.

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

Site de Destino

Selecione o site de destino para cópias de backup.

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. Sites que forem incluídos no IBM Spectrum Protect Plus, mas que não estiverem associados a um servidor vSnap não serão mostrados.

Utilizar apenas armazenamento em disco criptografado

Se o seu ambiente incluir servidores criptografados e não criptografados, marque esta caixa de seleção para fazer backup de dados para servidores vSnap criptografados.

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

7. Opcional: 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 [“Configurando parceiros de armazenamento de backup”](#) na página 120.

Replicação de armazenamento de backup

Selecione esta opção para ativar a replicação.

Esta opção é ativada apenas quando a **Política de backup** é selecionada.

Desativar Programação

Marque esta caixa de seleção para criar o relacionamento de replicação sem definir uma frequência ou horário de início. Este campo é opcional.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de replicação. Escolha entre **Minutos, Horas, Dias, Semanas, Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

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

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

Site de Destino

Selecione o site 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. Sites que forem incluídos no IBM Spectrum Protect Plus, mas que não estiverem associados a um servidor vSnap não serão mostrados.

Utilizar apenas armazenamento em disco criptografado

Selecione esta opção para replicar dados para servidores vSnap criptografados se o seu ambiente incluir servidores criptografados e não criptografados.

Restrição: Se esta opção for selecionada, mas nenhum servidor vSnap criptografado estiver 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.

8. Opcional: Na seção **Cópias Adicionais**, configure as opções para copiar dados para o armazenamento de objeto padrão ou armazenamento de objeto de archive.

Ao copiar dados de um servidor vSnap para o armazenamento em nuvem, a captura instantânea concluída com sucesso mais recente será copiada.

Armazenamento de objeto padrão (cópia incremental)

Selecione esta opção para copiar dados para o armazenamento em nuvem ou para um servidor do repositório. Esta opção é ativada apenas quando a **Política de backup** é selecionada.

Os dados são submetidos a backup para o servidor vSnap para proteção de curto prazo e, em seguida, copiados para o servidor de armazenamento em nuvem ou de repositório selecionado para proteção de longo prazo. Durante a primeira cópia de um volume de backup, é feito backup completo da captura instantânea. Depois que a primeira cópia da captura instantânea de base for concluída, as cópias subsequentes serão incrementais e capturarão mudanças acumulativas desde a última cópia. As operações de restauração do servidor em nuvem ou de repositório podem ser executadas a partir de qualquer servidor vSnap.

Desativar Programação

Marque esta caixa de seleção para criar o relacionamento de cópia sem definir uma frequência ou horário de início. Este campo é opcional.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de cópia. Escolha entre **Minutos**, **Horas**, **Dias**, **Semanas**, **Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

Insira a data e hora na qual deseja que a operação de cópia seja iniciada.

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

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.

Restrição: As opções de retenção de cópias serão desativadas se um servidor que usa a retenção Write Once Read Many (WORM) for selecionado no campo **Destino**.

Origem

Clique na origem para a operação de cópia:

Destino de política de backup

A origem para a operação de cópia é o site de destino que está definido na seção **Política de Backup**.

Destino da Política de Replicação

A origem para a operação de cópia é o site de destino que é definido na seção **Política de replicação**.

Esta opção será ativada apenas quando **Replicação de armazenamento de backup** for selecionado.

Destination

Clique em **Serviços de nuvem** ou **Servidores do repositório**.

Resposta

Clique no sistema de armazenamento em nuvem ou no servidor do repositório para o qual você deseja copiar dados.

Essa lista contém os sistemas de armazenamento secundário que você incluiu no IBM Spectrum Protect Plus..

Armazenamento de objeto de archive (cópia completa)

Selecione essa opção para arquivar dados no armazenamento em nuvem ou em um servidor do repositório para proteção de longo prazo. Esta opção é ativada apenas quando a **Política de backup** é selecionada.

Esta operação fornece uma cópia de imagem completa para o armazenamento de arquivo selecionado.

Desativar Programação

Marque esta caixa de seleção para criar o relacionamento de archive sem definir uma frequência ou horário de início. Este campo é opcional.

Frequência

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

Insira uma frequência para operações de archive. Escolha entre **Minutos, Horas, Dias, Semanas, Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.

Horário de Início

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

O fuso horário é preenchido automaticamente com as configurações do seu navegador. Para atualizar o fuso horário, clique no campo e selecione uma região e cidade a partir da lista, por exemplo: **Europa/Dublin**. Também é possível clicar no campo e entrar em uma região ou cidade no campo **Pesquisar** e selecionar um item dos resultados correspondentes.

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 de política de backup

A origem para a operação de archive é o site de destino que está definido na seção **Política de Backup**.

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**.

Esta opção será ativada apenas quando **Replicação de armazenamento de backup** for selecionado.

Destination

Clique em **Serviços de nuvem** ou **Servidores do 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.

9. Clique em **Salvar**.

A política de SLA que você criou é exibida na tabela na área de janela **Políticas de SLA**.

O que Fazer Depois

Depois de criar uma política de SLA, execute as seguintes ações:

- Designe permissões de usuário à política de SLA. Para obter instruções, consulte [“Criando uma função” na página 523](#).
- Crie uma definição de tarefa de backup que use a política de SLA. Para obter instruções, consulte [“Definindo backups de acordo de nível de serviço de volumes persistentes” na página 325](#).

Tarefas relacionadas

[“Editando uma política de SLA” na página 247](#)

Edite as opções para uma política de SLA para refletir mudanças no ambiente IBM Spectrum Protect Plus.

[“Excluindo uma política de SLA” na página 247](#)


Exclua uma política de SLA quando ela se tornar obsoleta.

Editando uma política de SLA

Edite as opções para uma política de SLA para refletir mudanças no ambiente IBM Spectrum Protect Plus.

Procedimento

Para editar uma política de SLA, 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 SLA** é exibida.
3. Edite as opções de política e, em seguida, clique em **Salvar**.

Excluindo uma política de SLA


Exclua uma política de SLA quando ela se tornar obsoleta.

Antes de Iniciar

Certifique-se de que não haja tarefas associadas à política de SLA.

Procedimento

Para excluir uma política de SLA, 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 SLA.

3. Clique em **Sim** para excluir a política.

4. Se você estiver excluindo a política de SLA demo, acesse **Configuração do Sistema > Site** e exclua o site chamado **Demo**.

Capítulo 10. Protegendo sistemas virtualizados

Você deve registrar os sistemas virtualizados que deseja proteger em IBM Spectrum Protect Plus e, em seguida, criar tarefas para fazer backup e restaurar os recursos que estão associados aos sistemas.

Os sistemas virtualizados referem-se a hypervisors VMware e Microsoft Hyper-V e a instâncias do Amazon EC2.

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.

Certifique-se de que o ambiente VMware atenda aos requisitos do sistema em [“Requisitos de restauração e backup do hypervisor \(Microsoft Hyper-V e VMware\) e da instância da nuvem \(Amazon EC2\)”](#) na página 40.

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 da máquina virtual para seu local original. Se você estiver restaurando uma máquina virtual para um local alternativo, a máquina virtual criptografada será restaurada sem criptografia e deve ser criptografada manualmente usando o vCenter Server após a conclusão da operação de restauração.

Os seguintes privilégios do vCenter Server são necessários para ativar operações para máquinas virtuais criptografadas:

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

Nota: Um volume NFS pode ser montado em qualquer número de data centers que pertencem ao mesmo vCenter. Se um volume do NFS estiver montado em mais de um data center, o vCenter tratará o mesmo volume como dois armazenamentos de dados diferentes. IBM Spectrum Protect Plus trata isso como um único armazenamento de dados e combina todas as VMs e VMDKs residindo no armazenamento de dados de todos os data centers nos quais o armazenamento de dados é montado. Qualquer seleção de SLA com relação a esse armazenamento de dados fará com que todas as VMs de diferentes data centers sejam submetidas a backup ou restauradas no IBM Spectrum Protect Plus.

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 > Sistemas Virtualizados > 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 SLA

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

6. Clique em **Save**. 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 523 .

Conceitos relacionados

[“Gerenciando identidades” na página 528](#)

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 253](#)

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 264](#)

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 (6.5 e 6.7)	<ul style="list-style-type: none"> • Incluir disco • Acesso direto • Criptografar • Criptografar novo • Gerenciar políticas de criptografia
Armazenamento de dados	<ul style="list-style-type: none"> • Alocar espaço • Procurar armazenamento de dados • Operações de arquivo de baixo nível • Remover de armazenamento de dados • Remover o arquivo • Atualizar arquivos da máquina virtual
Comutador Distribuído	<ul style="list-style-type: none"> • Operação de configuração de porta • Operação de configuração de porta
Pasta	<ul style="list-style-type: none"> • Criar pasta
Global	<ul style="list-style-type: none"> • Cancelar tarefa
Host > Configuração	<ul style="list-style-type: none"> • Configuração da partição de armazenamento
Serviço de Inventário > Identificação (6.0) vSphere Tagging (6.5, 6.7 e 7.0)	<ul style="list-style-type: none"> • Designar ou Remover Designação da Tag do vSphere • Designar ou Remover Designação de uma Tag do vSphere no Objeto (7.0) • 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
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 • Migrar máquina virtual desligada • Migrar máquina virtual ligada • Query vMotion

Objeto do vCenter Server	Privilégios Necessários
Máquina Virtual > Configuração	<ul style="list-style-type: none"> • Incluir disco existente • Incluir novo disco • Incluir ou remover dispositivo • Avançado (6.0 e 6.5) • Configuração avançada (6.7 e 7.0) • Mudar contagem de CPUs • Alterar memória (6.7 e 7.0) • Alterar configurações (7.0) • Configurar dispositivo bruto (6.7 e 7.0) • Rastreamento de mudança de disco (6.0 e 6.5) • Memória (6.0 e 6.5) • Modificar configurações do dispositivo • Dispositivo bruto (6.0 e 6.5) • Recarregar a partir do caminho • Remover disco • Renomear • Configurações (6.0, 6.5 e 6.7) • Alternar o rastreamento de mudança de disco (6.7 e 7.0)
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
Máquina Virtual > Interação	<ul style="list-style-type: none"> • Operação de backup na máquina virtual • Desligar • Ativado Ligado
Máquina Virtual > Inventário	<ul style="list-style-type: none"> • Registrar • Remover • Cancelar Registro
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 • Marcar como modelo • Marcar como máquina virtual
Máquina Virtual > Gerenciamento de Captura Instant	<ul style="list-style-type: none"> • Criar captura instantânea • Remover captura instantânea • Reverter captura instantânea

Objeto do vCenter Server	Privilégios Necessários
vApp	<ul style="list-style-type: none"> • Incluir máquina virtual • Designar conjunto de recursos • Designar vApp • Criar • Excluir • Desligar • Ativado Ligado • Renomear • Cancelar Registro • 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 > Sistemas Virtualizados > 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 Plus e a máquina virtual.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > 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 procedimentos e considerações a seguir antes de definir uma 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 249.
- Configure políticas do SLA. Para obter mais instruções, consulte [“Criar políticas de backup”](#) na página 163.
- 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 18, “Gerenciando o acesso de”,](#) na página 517.
- Se uma máquina virtual estiver associada a várias políticas de SLA, certifique-se de que as políticas não sejam planejadas para execução simultaneamente. Planeje as políticas de SLA para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de SLA.
- 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.
- Assegure-se de que a versão mais recente do VMware Tools esteja instalada em máquinas virtuais VMware.

Sobre Esta Tarefa

- Ao fazer backup de máquinas virtuais VMware, o IBM Spectrum Protect Plus faz o download dos arquivos .vmx, .vmxf e .nvram e, se necessário, os transfere para o servidor vSnap, conforme necessário. Para que isso ocorra com sucesso, o dispositivo IBM Spectrum Protect Plus deve ser capaz de resolver e acessar todos os hosts ESXi protegidos. Quando o dispositivo se comunicar com um host ESXi, o endereço IP correto deve ser retornado.
- Se uma VM for protegida por uma política de SLA, os backups da VM serão retidos com base nos parâmetros de retenção da política de SLA, mesmo se a VM for removida do vCenter.
- Se uma VM existente for migrada por uma operação de vMotion, IBM Spectrum Protect Plus executará uma operação de rebase se necessário.

Restrição: 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.

Procedimento

Para definir uma tarefa de backup do VMware, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > 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 SLA** para incluir uma ou mais políticas de SLA que atendam aos seus critérios de backup para a definição de tarefa.
4. Para criar a definição de tarefa usando opções padrão, clique em **Salvar**.

A tarefa será executada conforme definido pelas políticas de SLA que você selecionou. Para executar a tarefa imediatamente, clique em **Tarefas e operações > Planejamento**. Selecione a tarefa e clique em **Ações > Iniciar**.

Dica: Quando a tarefa para a política de SLA selecionada é executada, todos os recursos que estão associados a essa política de SLA são incluídos na operação de backup. Para fazer backup apenas de recursos selecionados, é possível executar uma tarefa on demand. Uma tarefa sob demanda executa a operação de backup imediatamente.

- Para executar uma tarefa de backup on demand para um único recurso, selecione o recurso e clique em **Executar**. Se o recurso não estiver associado a uma política de SLA, o botão **Executar** não estará disponível.
- Para executar uma tarefa de backup on demand para um ou mais recursos, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.

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 SLA que a máquina virtual. Se desejar uma operação de backup mais granular, será possível excluir VMDKs individuais da política de SLA. Para obter instruções, consulte [“Excluindo VMDKs da política de SLA para uma tarefa”](#) na página 258.

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. Se um valor de prioridade não for configurado, uma prioridade de cinco será configurada por padrão.

Na seção **Opções de captura instantânea**, configure as seguintes opções de definição de tarefa:

Tornar o aplicativo de captura instantânea/sistema de arquivos 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 Repetição da Captura Instant

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.

Recuar para a captura instantânea fora 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:

Truncar 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 login do sistema deve ter as seguintes permissões:

- As permissões do SQL Server sysadmin 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 a tarefa de backup e o truncamento de 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 em que ocorreu o truncamento do log.

Restrição: A indexação de arquivo e a restauração de arquivo não são suportadas por meio dos pontos de restauração que foram copiados 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 **Guest OS Username** e **Guest OS Password** dentro da 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.

Restrição: As Chaves SSH não são um mecanismo de autorização válido para plataformas Windows.

Arquivos de Exclusão

Insira diretórios a serem ignorados durante a indexação de arquivo. 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.


Nome de Usuário/Senha do OS Guest

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 e, em seguida, clique em **Selecionar Opções**. Selecione **Usar o usuário existente** e selecione um nome do usuário e uma senha inseridos anteriormente para o recurso e, em seguida, clique em **Testar**.

7. Clique **Salvar**.

8. Para configurar opções adicionais, clique no ícone de área de transferência **Opções de Política**  que está associado à tarefa na seção **Status da Política de SLA**. Configure as opções de política adicionais a seguir:

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.

Excluir Recursos

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 260.
Crie uma definição de tarefa de restauração do VMware.	Consulte “Restaurando Dados do VMware” na página 264.

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.](#)

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração” na página 504](#)

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 sob demanda” na página 497](#)

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Excluindo VMDKs da política de SLA 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 SLA que está designada à tarefa.

Antes de Iniciar

Excluir um ou mais VMDKs de uma operação de backup pode impactar o sucesso da recuperação. Considere os cenários a seguir antes de excluir um disco de uma operação de backup da VM.

- Para Instant Disk Restore, se um VMDK for selecionado para uma operação de restauração, uma VM existente é escolhida como o destino. IBM Spectrum Protect Plus monta o disco restaurado para a VM de destino escolhida.
- Para Instant VM Restore, se o VMDK que foi excluído durante um backup contiver dados que são necessários para inicializar a máquina virtual, então a VM restaurada pode falhar na inicialização.
- Para VMs com guests baseados em Windows, a VM restaurada pode falhar ao inicializar se o disco no qual o sistema operacional principal estiver instalado, normalmente a unidade C :, foi excluído durante a operação de backup.
- Para VMs com guests baseados em Linux, a VM restaurada pode falhar:
 - Se um disco que contém a inicialização ou a partição raiz foi excluído durante o backup.
 - Se um disco contendo uma partição de dados (não raiz) foi excluído durante o backup, e o volume de dados não tiver a opção 'nofail' especificada no /etc/fstab, então a VM restaurada poderá falhar.

Procedimento

Para excluir VMDKs da política de SLA:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > 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 SLA**.
5. Desmarque a caixa de seleção para a política de SLA 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.

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 de tarefas livres. As tarefas livres são determinadas pelo número de núcleos da CPU disponíveis ou usando a opção **Limite leve de tarefas**.

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 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 é preferencial em um ambiente de armazenamento direto porque geralmente ele é rápido e confiável.
- O modo de transporte HotAdd é preferencial se o proxy VADP for virtualizado. Esse modo suporta todos os tipos de armazenamento do vSphere.

Nota: Para usar apenas o modo de transporte HotAdd sem recuar para os modos de transporte alternativos, selecione **Proxy VADP usa apenas o modo de transporte HotAdd** em **Preferências Globais**. Para obter mais informações, consulte [“Configurando preferências globais”](#) na página 222.

- Modo de transporte NBD ou NBDSSL (LAN) é o modo de fallback porque funciona em ambientes físicos, virtuais e mistos. No entanto, com esse modo, a velocidade da transferência de dados pode ser 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

Revise os requisitos do sistema IBM Spectrum Protect Plus em [“Requisitos do proxy do VADP”](#) na página 33.

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 523.

Restrição: Para executar as etapas para criar proxies VADP, assegure-se de que você tenha um ID do usuário com a função SYSADMIN atribuída. Para obter mais informações sobre funções, consulte [“Gerenciando atribuições”](#) na página 521.

Dica: 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**.
5. Clique em **Sim** na tela de confirmação.
6. Repita as etapas anteriores para cada proxy que você deseja criar.

Resultados

O proxy é incluído na tabela **Proxy VADP**. Você pode suspender, desinstalar, cancelar o registro ou editar um servidor proxy clicando no ícone de reticências **...** para abrir o menu de 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 retomar o uso do proxy, clique no ícone de reticências **...** para abrir o menu de ações e clique em **Retomar**. Após a criação bem-sucedida, o vadp de serviço é iniciado na máquina proxy. Um arquivo de log, `vadp.log`, é gerado no diretório `/opt/IBM/SPP/logs`.

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. Emita o comando a seguir: `ping <vadp_ip>`, em que `<vadp_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, assegure-se de que haja uma conexão adequada do proxy VADP com o dispositivo virtual IBM Spectrum Protect Plus executando o procedimento a seguir:

1. Conecte-se à linha de comandos para o proxy VADP usando o protocolo de rede Shell Seguro (SSH).
2. Emita o comando a seguir: `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, é possível concluir a seguinte ação:

Ação	Como
Execute a tarefa de backup do VMware.	<p>Consulte “Fazendo backup dos dados de VMware” na página 253.</p> <p>Os proxies são indicados no log da tarefa por uma mensagem de log semelhante ao seguinte texto:</p> <pre>Run remote vmdkbackup of MicroService: http://<proxy> nodename, IP:proxy_IP_address</pre>

Tarefas relacionadas

“Configurando Opções para Proxies VADP” na página 263

Quando você cria proxies VADP no IBM Spectrum Protect Plus, é possível configurar várias opções para cada proxy VADP.

Registrando um proxy VADP em um servidor vSnap

É possível instalar e registrar um proxy VADP em um servidor vSnap físico ou virtual. Ao instalar e registrar um proxy VADP em um servidor vSnap, você pode ajudar a otimizar o movimento de dados eliminando uma montagem do NFS porque os dois sistemas estão na mesma máquina.

Antes de Iniciar

Um ou mais servidores de vSnap independentes devem ser devidamente implementados e configurados em seu ambiente e incluídos em provedores de armazenamento de backup IBM Spectrum Protect Plus. Para obter instruções, consulte [“Registrando um servidor vSnap como um provedor de armazenamento de backup” na página 115.](#)


Para os requisitos de sistema combinados de um servidor vSnap e do proxy do VADP, consulte [Proxy do VADP em requisitos do servidor vSnap.](#)

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 523.](#)

A identidade associada a um servidor vSnap é a conta que é usada para registrar o proxy VADP no servidor vSnap. Ao registrar um proxy VADP em um servidor vSnap, um instalador é enviado e requer privilégios sudo para instalar com sucesso o software de proxy VADP. A identidade associada a um servidor vSnap deve ter privilégios sudo.

Dica: Use o ID do Usuário serveradmin ao incluir um servidor vSnap no IBM Spectrum Protect Plus. Ao implementar um proxy VADP em um servidor vSnap, é usada essa conta que já possui todos os privilégios necessários.

Procedimento

1. Na área de janela de navegação, em **Configuração do Sistema > Armazenamento de Backup > Disco.** Os servidores vSnap disponíveis são exibidos na tabela na área de janela de Armazenamento em Disco.
2. Selecione o servidor vSnap no qual o proxy VADP deve ser instalado e registrado.
3. Clique no ícone do menu de ações . Selecione **Registrar como Proxy VADP.**
4. Na caixa de diálogo Confirmar, clique em **Sim.**

Resultados

Quando o processo estiver concluído, um visto verde aparecerá na coluna **Proxy VADP** na tabela da área de janela Armazenamento em Disco.

Configurando Opções para Proxies VADP

Quando você cria proxies VADP no IBM Spectrum Protect Plus, é possível configurar várias opções para cada proxy VADP.

Antes de Iniciar

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 523](#).

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 proxy VADP que você deseja configurar, que, em seguida, exibe as informações na área de janela de detalhes adjacente.
3. Na área de janela de detalhes do proxy VADP, clique no ícone de reticências **...** e, em seguida, escolha **Opções de Proxy**.
4. Preencha os seguintes campos na área de janela **Configurar opções de proxy VADP**:

Site

Designa um site para o proxy.

Usuário

Selecione um nome de usuário inserido anteriormente para o provedor.

Modos de Transporte (lista ordenada)

Configure os modos de transporte a serem usados pelo proxy. A ordem na qual cada modo é selecionado determinará a ordem na qual os modos de transporte serão usados. Para remover um modo de transporte, clique no ícone excluir ao lado do modo de transporte. 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. Os tipos de compactação disponíveis incluem **libz**, **fastlz** e **skipz**.

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 configurar as opções de proxy VADP, é possível concluir as seguintes ações:

Ação	Como
Execute a tarefa de backup do VMware.	Consulte “Fazendo backup dos dados de VMware” na página 253.
Desinstale os proxies quando você deixar de executar as tarefas de backup do VMware.	Consulte “Desinstalando proxies VADP” na página 264.

Tarefas relacionadas

“Criando proxies do VADP” na página 260

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:

Nota: Este procedimento só se aplica aos proxies VADP que foram instalados no ambiente. Ele não se aplica ao proxy VADP que é implementado com o dispositivo IBM Spectrum Protect Plus.

1. Na área de janela de navegação, clique em **Configuração do Sistema > Proxy VADP**.
2. Clique no proxy VADP que deseja desinstalar, que então exibe as informações na área de janela de detalhes adjacente.
3. Clique no ícone de reticências **...** na área de janela de detalhes e selecione **Desinstalar**.

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 253.
- Assegure-se de que funções apropriadas sejam designadas a usuários do IBM Spectrum Protect Plus para que eles possam concluir operações de backup e restauração. Conceda aos usuários acesso a hypervisors e a operações de backup e restauração por meio da área de janela **Contas**. Para obter mais informações, consulte Capítulo 18, [“Gerenciando o acesso de”](#), na página 517 e [“Gerenciando contas do usuário”](#) na página 526.
- 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.
- Ao restaurar uma máquina virtual usando o modo de clone e usando a configuração de IP original, assegure-se de que as credenciais sejam estabelecidas por meio das opções **Nome do usuário do S.O. de guest** e **Senha do S.O. de guest** dentro da definição de tarefa de backup.

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 271.

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.

O tamanho de uma máquina virtual restaurada a partir de uma cópia 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 operação de cópia. O tamanho padrão dos dados deve ser transferido, mesmo que não esteja alocado na máquina virtual de origem.

Ao restaurar dados do VMware a partir de um arquivo IBM Spectrum Protect, os arquivos inicialmente serão migrados da fita para um conjunto temporário. Dependendo do tamanho da operação de restauração, esse processo pode levar várias horas.

Restrição: A indexação e a restauração de arquivos do Windows em volumes que residem em discos dinâmicos não são suportadas.

Procedimento



Para definir uma tarefa de restauração do VMware, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > VMware > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restauração > VMware**.
- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
- O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.

2. Na página **Selecionar origem**, tome 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**, selecione o tipo de tarefa de restauração que você deseja criar:
- On Demand**
Executa uma operação de restauração única. 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.
4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar. Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma restauração de recurso único on demand

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão.

Opção	Descrição
	Por exemplo, se os tipos de armazenamento Backup , Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração múltipla de recursos ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

5. Na página **Configurar Destino**, especifique a instância que você gostaria de restaurar para cada origem escolhida e clique em **Avançar**:

Host ou cluster original

Selecione esta opção para restaurar dados para o host ou cluster original.

Host ou cluster 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 ignorar o vCenter Server e para restaurar dados diretamente em um host ESXi. Em outros cenários de restauração, as ações são concluídas por meio do vCenter Server. Se o vCenter Server estiver indisponível, essa opção restaura a máquina virtual ou as máquinas virtuais que contêm os componentes de que o vCenter Server depende.

Ao selecionar um host ESXi, você deve especificar o usuário do host. É possível selecionar um usuário existente para o host ou criar um novo.

Para criar um usuário, insira um nome de usuário, o ID do usuário e a senha do usuário.

Se o host ESXi estiver conectado a um domínio, o ID do usuário seguirá o formato padrão *domain \name*. Se o usuário for um administrador local, use o formato *local_administrator*.

Para restaurar dados para um host ESXi, o host deve ter um comutador padrão ou um comutador distribuído com ligação efêmera. Revise as informações em [“Restaurando dados quando o vCenter Server ou outras VMs de gerenciamento não estiverem acessíveis” na página 273](#) para garantir que você tenha o ambiente correto configurado para usar esta opção.

6. Na página **Configurar armazenamento de dados**, execute as ações a seguir:

- Se você estiver restaurando dados para um host ou cluster do ESXi alternativo, selecione o armazenamento de dados de destino e clique em **Avançar**.
 - Se você estiver restaurando dados para o host ou cluster do ESXi original, esta página não será exibida.
7. 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 para o host ou cluster do ESXi 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 esta opção para restaurar dados para o host ou cluster original usando sua configuração de endereço IP predefinido. 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 para um host ou cluster do ESXi 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.

Nota: Quando um mapeamento é incluído, o endereço IP de origem deve ser inserido no campo pelo botão **+**. As informações de endereço IP de destino devem ser inseridas nos

campos **Sub-rede / Endereço IP, Máscara de Sub-rede e Gateway**. O reendereçamento só pode ser feito em máquinas com VMware Tools instaladas antes da execução da tarefa de backup que deve ser restaurada.

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.

8. Na página **Métodos de Restauração**, selecione o método de restauração a ser usado para seleção de origem. Configure a tarefa de restauração do VMware para executar em modo de teste, produção ou clone. 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.
9. Se você estiver executando a tarefa de restauração no modo avançado, será possível configurar opções adicionais como segue:

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.

Restaurar tags VM

Ative esta opção para restaurar tags que são aplicadas às máquinas virtuais por meio do vSphere.

Ativar restauração de fluxo (VADP)

O fluxo paralelo para operações de restauração de máquina virtual é configurado por padrão. É possível desmarcar essa opção para operações de restauração da máquina virtual.

Dica: Quando você está restaurando máquinas virtuais gerenciadas por um VMware Cloud (VMC) no AWS Software-Defined Data Center (SDDC), essa opção deve sempre ser ativada para permitir o fluxo dos dados.

Anexar Sufixo ao Nome da Máquina Virtual

Insira um sufixo a ser incluído nos nomes de máquinas virtuais restauradas.

Prependendo prefixo para nome da máquina virtual

Insira um prefixo a ser incluído nos nomes de máquinas virtuais restauradas.

10. 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.

11. 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**.

12. 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 da Tarefa 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 249

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 264.

Procedimento

Para criar uma rede protegida, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > 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 249

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 Server ou outras VMs de gerenciamento não estiverem acessíveis

IBM Spectrum Protect Plus fornece uma opção para restaurar dados automaticamente usando um host ESXi se o vCenter Server ou um dos componentes que ele usa não estiverem acessíveis. Essa opção restaura as máquinas virtuais que contêm os componentes que o vCenter Server utiliza.

Antes de Iniciar

Para concluir este procedimento, você deve estar familiarizado com as interfaces com o usuário do ESXi e do vCenter Server.

Sobre Esta Tarefa

O vCenter Server usa os seguintes componentes:

- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)

- Active Directory (AD)
- Servidores de Sistema de Nomes de Domínio (DNS)

Para usar a opção **ESX host if vCenter is down**, o host ESXi deve ter um comutador padrão ou um comutador distribuído. O comutador distribuído deve ter ligação efêmera. Se um ou ambos os comutadores estiverem disponíveis, será possível executar uma operação de restauração no IBM Spectrum Protect Plus com a opção ativada, conforme descrito em [“Restaurando Dados do VMware” na página 264](#), e nenhuma configuração manual adicional será necessária.

Se nenhum desses comutadores estiver disponível, você deverá concluir as etapas a seguir antes de poder usar a opção **ESX host if vCenter is down**.

Procedimento

1. Conecte-se à interface com o usuário do host ESXi de destino e crie um comutador virtual padrão. O novo comutador não possui grupos de porta ou uplinks.

2. Use o protocolo Shell Seguro (SSH) para conectar-se ao host ESXi.

3. Liste os comutadores distribuídos que estão configurados no host ESXi emitindo o seguinte comando:

```
#esxcli network vswitch dvs vmware list
```

4. Identifique a placa da interface de rede (NIC) física e o grupo de portas do comutador distribuído que você deseja utilizar para a operação de restauração.

5. Remova a NIC física e o grupo de portas do comutador distribuído emitindo o seguinte comando:

```
#esxcfg-vswitch -Q physical_vnic -V port_group switch_name
```

6. Inclua a NIC física e o grupo de portas no novo comutador padrão emitindo o comando a seguir:

```
#esxcli network vswitch standard uplink add --uplink-name=physical_vnic --vswitch-name=new_standard_vswitch
```

7. Na interface com o usuário do host ESXi, inclua um grupo de portas temporárias e selecione o comutador padrão que você criou na etapa [“1” na página 274](#).

O comutador padrão possui um grupo de portas e um uplink.

8. Execute uma operação de restauração em IBM Spectrum Protect Plus com a opção **Host ESX se o vCenter estiver desativado** ativada.

Para obter instruções sobre como executar uma operação de restauração, consulte [“Restaurando Dados do VMware” na página 264](#).

9. Na interface com o usuário do host ESXi para o host ESXi, ligue as VMs que são restauradas.

10. Efetue login na interface com o usuário do vCenter Server e inicie a migração das VMs de gerenciamento do grupo de portas temporárias que você criou na etapa [“7” na página 274](#) para um grupo de portas distribuídas disponível.

11. Depois que todas as VMs forem migradas para o grupo de portas original, reincorpore a NIC física e o grupo de portas no comutador distribuído original, tomando as seguintes ações. Por exemplo, os comandos a seguir fazem referência a uma placa da interface de rede (VNIC) virtualizada denominada vmnic0 que faz parte do grupo de portas 64.

- a. Remova as placas de rede (conhecidas como vmnics) de um comutador padrão emitindo o comando a seguir:

```
#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 no comutador distribuído emitindo o comando a seguir:


```
#esxcfg-vswitch -P vmnic -V unused_distributed_switch_port_ID distributed_switch
```

Por exemplo:

```
#esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
```

12. Exclua o grupo de portas temporárias e o comutador padrão da interface com o usuário do host ESXi.
13. Depois que as VMs forem migradas e estiverem acessíveis, use a interface com o usuário do host ESXi para cancelar o registro das, mas não excluir as, 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**. Essa opção cancela o registro de uma VM do catálogo do vCenter Server, mas deixa arquivos VMDK no armazenamento de dados em que os arquivos consomem espaço de armazenamento. 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 de restauração e backup do hypervisor (Microsoft Hyper-V e VMware) e da instância da nuvem (Amazon EC2)” na página 40.

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 > Sistemas Virtualizados > 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.

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 276](#).

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 523 .

Tarefas relacionadas

[“Fazendo Backup de Dados do Hyper-V” na página 277](#)

Use uma tarefa de backup para fazer backup de dados do Hyper-V com capturas instantâneas.

[“Restaurando dados do Hyper-V” na página 281](#)

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 comando 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 > Sistemas Virtualizados > 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 Plus e a máquina virtual.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > 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

Revise os procedimentos e considerações a seguir antes de definir uma tarefa de backup:

- Registre os provedores dos quais você deseja fazer backup. Para obter mais informações, consulte [“Incluindo um servidor Hyper-V” na página 275](#)
- Configure políticas do SLA. Para obter instruções, consulte [“Criar políticas de backup” na página 163](#).
- 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 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 18, “Gerenciando o acesso de”](#), na página 517.
- Se uma máquina virtual estiver associada a várias políticas de SLA, certifique-se de que as políticas não estejam planejadas para execução simultaneamente. Planeje as políticas de SLA para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de SLA.
- 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 SLA, os backups da VM serão retidos com base nos parâmetros de retenção da política de SLA, mesmo se a VM for removida.

Sobre Esta Tarefa

Restrição: 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.

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 > Sistemas Virtualizados > 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 SLA** para incluir uma ou mais políticas de SLA que atendam aos seus critérios 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: Quando a tarefa para a política de SLA selecionada é executada, todos os recursos que estão associados a essa política de SLA são incluídos na operação de backup. Para fazer backup apenas de recursos selecionados, é possível executar uma tarefa on demand. Uma tarefa sob demanda executa a operação de backup imediatamente.

- Para executar uma tarefa de backup on demand para um único recurso, selecione o recurso e clique em **Executar**. Se o recurso não estiver associado a uma política de SLA, o botão **Executar** não estará disponível.
 - Para executar uma tarefa de backup on demand para um ou mais recursos, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.
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 Hyper-V** 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. Se um valor de prioridade não for configurado, uma prioridade de cinco será 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 Repetição da Captura Instant

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:

Truncar 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 copiados 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 o usuário existente** e selecione um nome do usuário e uma senha inseridos anteriormente para o recurso e, em seguida, clique em **Testar**.

7. Clique **Salvar**.
8. Para configurar opções adicionais, clique no campo **Opções de política** que está associado à tarefa na seção **Status de política de SLA**. 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.

Excluir Recursos

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 281.

Conceitos relacionados

“Configurando scripts para operações de backup e restauração” na página 504

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 sob demanda” na página 497

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 277.
- 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 18, “Gerenciando o acesso de”](#), na página 517 e [“Gerenciando contas do usuário”](#) na página 526.
- 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.
- Ao restaurar uma máquina virtual usando o modo de clone e usando a configuração de IP original, assegure-se de que as credenciais sejam estabelecidas por meio das opções **Nome do usuário do S.O. de guest** e **Senha do S.O. de guest** dentro da definição de tarefa de backup.

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 > Sistemas Virtualizados > Hyper-V > Criar Tarefa**, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.


Dicas:


- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Hyper-V**.
- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
- O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.

2. Na página **Selecionar origem**, tome 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On Demand

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma restauração de recurso único on demand

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none">• Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <p>Backup Restaura dados que são submetidos a backup para um servidor vSnap.</p> <p>Replicação Restaura dados que são replicados para um servidor vSnap.</p>

Opção	Descrição
	<p>Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório.</p> <p>Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).</p> <ul style="list-style-type: none"> • Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração múltipla de recursos ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>
Selecione um local	Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:

Opção	Descrição
	<p>Demo O site de demonstração do qual restaurar capturas instantâneas.</p> <p>Primário O site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

5. Na página **Configurar destino**, escolha a instância a ser restaurada para a origem selecionada e clique em **Avançar**:

Host ou cluster original

Selecione esta opção para restaurar dados para o host ou cluster original.

Host ou cluster 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.

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.

6. 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 para o host ou cluster original do Hyper-V, esta página não será exibida.

7. 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.

Nota: Quando um mapeamento é incluído, o endereço IP de origem deve ser inserido no campo pelo botão **+**. As informações de endereço IP de destino devem ser inseridas nos campos **Sub-rede / Endereço IP, Máscara de Sub-rede e Gateway**. O reendereçamento só pode ser feito em máquinas com VMware Tools instaladas antes da execução da tarefa de backup que deve ser restaurada.

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.

8. 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.

9. 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.

10. 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.

11. 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**.
12. 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 277](#)

Use uma tarefa de backup para fazer backup de dados do Hyper-V com capturas instantâneas.

[“Incluindo um servidor Hyper-V” na página 275](#)

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.

Fazendo backup e restaurando dados do Amazon EC2

Para proteger os dados do Amazon EC2, primeiro inclua uma conta para suas instâncias EC2 em IBM Spectrum Protect Plus e, em seguida, crie tarefas para operações de backup e restauração para essas instâncias.

Para incluir uma conta EC2 em IBM Spectrum Protect Plus, as chaves de acesso são necessárias. As chaves de acesso são credenciais de longo prazo para um usuário do usuário do Identity and Access Management (IAM) ou usuário raiz da conta do Amazon Web Services (AWS).

Para obter informações sobre como criar um usuário do IAM com chaves de acesso e as permissões que são necessárias para IBM Spectrum Protect Plus, consulte [“Criando um usuário do AWS IAM ” na página 288](#).

Para o aumento da segurança, é recomendado que o usuário raiz da conta do AWS não seja usado para IBM Spectrum Protect Plus. Para obter mais informações sobre o usuário raiz, consulte o [Guia do Usuário do AWS Identity and Access Management](#).

Os dados do EC2 são armazenados em capturas instantâneas do Amazon Web Services (AWS) Elastic Block Store (EBS) em vez do servidor vSnap. O IBM Spectrum Protect Plus gerencia essas capturas instantâneas para operações de backup e restauração.

Assegure-se de que seu ambiente EC2 atenda aos requisitos do sistema em [“Requisitos de restauração e backup do hypervisor \(Microsoft Hyper-V e VMware\) e da instância da nuvem \(Amazon EC2\) ” na página 40](#).

Criando um usuário do AWS IAM

Para concluir tarefas na interface com o usuário do IBM Spectrum Protect Plus, os usuários do IAM devem ter chaves de acesso e permissões necessárias.

Sobre Esta Tarefa

É possível usar o AWS Management Console para criar um usuário do IAM usando as etapas a seguir. Essas etapas são condensadas a partir das etapas que estão documentadas no [Guia do Usuário do AWS Identity and Access Management](#) para mostrar configurações que são necessárias para IBM Spectrum Protect Plus. Para obter as etapas completas e detalhadas para criação de um usuário do IAM, consulte este guia.

Para criar um usuário, você deve ter permissões administrativas do IAM.

Procedimento

1. Conecte-se ao [Console de Gerenciamento do AWS](#) e clique em **Serviços > IAM** para abrir o Console de Gerenciamento do IAM.
2. Na área de janela de navegação do console, clique em **Usuários > Incluir usuário**.
3. Digite o nome do usuário para o novo usuário.
4. Selecione **Acesso programático** para o tipo de acesso AWS.
Esse tipo de acesso é necessário para criar uma chave de acesso, que é requerida pelo IBM Spectrum Protect Plus. IBM Spectrum Protect Plus não requer o tipo de acesso **Acesso do AWS Management Console**.
5. Clique em **Avançar: permissões**.
6. Clique em **Anexar Políticas Existentes Diretamente** e, em seguida, clique em **Criar Política**.
A página **Criar política** é aberta em uma nova janela do navegador.
7. Clique na guia **JSON** e insira as ações a seguir:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:CreateVolume",
        "ec2:DescribeTags",
        "ec2:CreateTags",
        "ec2:RegisterImage",
        "ec2:DescribeRegions",
        "ec2:RunInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateSnapshots",
        "ec2:DescribeVolumes",
        "ec2:CreateSnapshot",
        "ec2:DescribeSubnets",
        "iam:PassRole"
      ],
      "Resource": "*"
    }
  ]
}
```

8. Clique em **Revisar política**.
9. Digite um nome e uma descrição (opcional) para a política que você está criando.
10. Revise a seção **Resumo** para ver as permissões que são concedidas pela política.
11. Clique em **Criar política**.
12. Feche a janela do navegador e retorne para a janela que contém a página **Incluir Usuário**.
13. Selecione a política que você criou a partir da lista de políticas.
14. Opcional: Configure um limite de permissões.
15. Clique em **Avançar: tags**.

16. Opcional: Inclua metadados no usuário anexando tags como pares chave-valor.
É possível usar tags para filtrar recursos ao fazer backup ou restaurar dados EC2.
17. Clique em **Avançar: Revisar**.
18. Revise suas escolhas e, em seguida, clique em **Criar usuário**.
Uma nova janela é aberta mostrando o nome do usuário, a chave de acesso e a chave secreta.
19. Para visualizar a chave secreta, clique em **Mostrar** ao lado da chave secreta.
20. Clique em **Download.csv** para salvar o ID da chave de acesso e a chave de acesso secreto a um arquivo CSV em seu computador.
Armazene o arquivo em um local seguro. Não é possível acessar a chave de acesso secreto novamente depois que essa caixa de diálogo fechar.
21. Clique em **Fechar** para fechar a janela.

O que Fazer Depois

Inclua uma conta para EC2. Para criar uma conta, siga as instruções em [“Incluindo uma conta do Amazon EC2”](#) na página 290.

Incluindo uma conta do Amazon EC2

Quando uma conta do Amazon EC2 é incluída no IBM Spectrum Protect Plus, um inventário das instâncias que estão associadas à conta é capturado. Em seguida, é possível executar tarefas de backup e de restauração e gerar relatórios para as instâncias.

Antes de Iniciar

Uma chave de acesso é necessária para incluir uma conta EC2. A chave de acesso permite que IBM Spectrum Protect Plus se conecte e faça o inventário de instâncias EC2 para proteção de dados. As chaves de acesso que já estão inseridas em IBM Spectrum Protect Plus são fornecidas em uma lista de seleção. Se a chave de acesso que você deseja usar não estiver na lista, deve-se adicionar a chave de acesso e a chave de segurança. Assegure-se de que você tenha a chave de acesso e chave secreta que você deseja incluir.

Procedimento

Para incluir uma conta EC2, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > Amazon EC2**.
2. Clique em **Gerenciar Contas**.
3. Clique em **Incluir Conta**.
4. Preencha os campos na seção **Propriedades da Conta**:

Número da conta

Insira um nome significativo para identificar a chave de acesso que você seleciona para a conta.

Usar chave de acesso existente

Para especificar uma chave de acesso inserida anteriormente para a conta, selecione esta opção e, em seguida, selecione a chave na lista **Selecionar uma Chave**.

Se você não selecionar esta opção, preencha os campos a seguir para incluir uma chave.

Chave de Acesso

Insira a chave de acesso.

Chave Secreta

Insira a chave secreta.

5. Clique em **Save**.

IBM Spectrum Protect Plus confirma uma conexão de rede, inclui a conta EC2 no banco de dados e, em seguida, cataloga as instâncias da conta.

Se uma mensagem indicar que a conexão não foi bem-sucedida, revise suas entradas. Se as suas entradas estiverem corretas e a conexão não for bem-sucedida, entre em contato com um administrador de rede para revisar a conexão.

O que Fazer Depois

Ao incluir uma conta EC2 em IBM Spectrum Protect Plus, um inventário é executado automaticamente em cada instância que está associada à conta. As instâncias devem ser detectadas para garantir que elas possam ser submetidas a backup. É possível executar um inventário manual a qualquer momento para detectar atualizações. Para obter instruções sobre como executar um inventário manual, consulte [“Detectando instâncias do Amazon EC2” na página 291](#).

Tarefas relacionadas

[“Fazendo backup de dados do Amazon EC2” na página 291](#)

Use uma tarefa de backup para fazer backup de dados em uma instância do Amazon EC2.

[“Restaurando dados do Amazon EC2” na página 293](#)

Use uma tarefa de restauração para restaurar dados do EC2 a partir de uma cópia de backup. Por exemplo, se os dados em uma instância forem perdidos ou corrompidos. É possível definir uma tarefa que restaure dados para a zona de disponibilidade original ou para uma zona de disponibilidade diferente na mesma região, com diferentes tipos de opções de recuperação e configurações disponíveis.

Detectando instâncias do Amazon EC2

As instâncias da Amazon EC2 são automaticamente detectadas após uma conta EC2 ser incluída em IBM Spectrum Protect Plus. No entanto, é possível executar uma tarefa de inventário para detectar quaisquer mudanças que ocorreram desde que a conta foi incluída.

Procedimento

Para executar uma tarefa de inventário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > Amazon EC2**.
2. Na lista de contas EC2, selecione uma conta ou contas ou clique no link para uma conta para navegar para as regiões ou instâncias das quais você deseja fazer o inventário.
A navegação está na conta de ordem> região> instância.
3. Clique em **Executar Inventário**.

Fazendo backup de dados do Amazon EC2

Use uma tarefa de backup para fazer backup de dados em uma instância do Amazon EC2.

Antes de Iniciar

Execute as seguintes etapas:

1. Certifique-se de que as contas a serem submetidas a backup sejam incluídas em IBM Spectrum Protect Plus. Para obter mais instruções, consulte [“Incluindo uma conta do Amazon EC2” na página 290](#).
2. Assegure-se de que uma ou mais políticas de SLA estejam configuradas para as instâncias do EC2. Para obter mais instruções, consulte [“Criando uma política de SLA para instâncias do Amazon EC2” na página 241](#).
3. Assegure-se de que as funções e os grupos de recursos do IBM Spectrum Protect Plus estejam designados para o usuário que estiver configurando a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 18, “Gerenciando o acesso de”, na página 517](#).
4. Se uma conta estiver associada a múltiplas políticas de SLA, assegure-se de que as políticas não estejam planejadas para serem executadas 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.

Procedimento

Para definir uma tarefa de backup do EC2, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > Amazon EC2**.
2. Selecione as instâncias para fazer backup na área de janela Backup do Amazon EC2 tomando uma das seguintes ações:
 - Para selecionar todas as instâncias que estão associadas a uma conta EC2, marque a caixa de seleção para a conta. Quaisquer instâncias incluídas nessa conta são designadas automaticamente à política de SLA que você escolher.
 - Para selecionar instâncias por região ou instâncias específicas, clique no nome da conta e navegue para a região ou instância. A navegação está na conta de ordem > região > instância. Se uma instância não tiver um nome atribuído, o ID da instância será mostrado como o nome da instância.

Para procurar instâncias disponíveis, use a função de procura e alterne as instâncias exibidas usando o filtro **Visualizar**. As opções disponíveis são **Instâncias** e **Tags**.

3. Clique em **Selecionar Política de SLA** para incluir uma ou mais políticas de SLA que atendam aos seus critérios de backup para a definição de tarefa a partir da tabela **Status de Política de SLA**.
4. Opcional: Para configurar opções adicionais para as políticas de SLA que você adicionou à definição, na coluna **Opções de Política** da tabela **Status de Política de SLA**, clique no ícone da área de

transferência para uma política de SLA  e configure as opções a seguir.

Se a tarefa já estiver configurada, clique no ícone para editar a configuração.

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 em Windows suportam scripts em lote e do PowerShell enquanto as máquinas baseadas em 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 que está associado à tarefa falhar, selecione **Continuar atividade/tarefa no erro de 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 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 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 das instâncias selecionadas antes de iniciar a tarefa de backup.

Excluir Recursos

Excluir instâncias específicas 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.

5. Clique em **Salvar** para criar a definição de tarefa.

A tarefa será executada conforme definido pelas políticas de SLA que você selecionou. Para executar a tarefa imediatamente, clique em **Tarefas e operações > Planejamento**. Selecione a tarefa e clique em **Ações > Iniciar**.

Dica: Quando a tarefa para a política de SLA selecionada é executada, todas as instâncias que estão associadas a essa política de SLA são incluídas na operação de backup. Para fazer backup apenas de instâncias selecionadas, é possível executar uma tarefa on demand. Uma tarefa on demand executa a operação de backup imediatamente.

- Para executar uma tarefa de backup on demand para uma única instância, selecione a instância e clique em **Executar**. Se o recurso não estiver associado a uma política de SLA, o botão **Executar** não estará disponível.
- Para executar uma tarefa de backup on demand para uma ou mais instâncias, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.

O que Fazer Depois

Depois de definir uma tarefa de backup do EC2, crie uma definição de tarefa de restauração do EC2.

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração”](#) na página 504

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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

[“Restaurando dados do Amazon EC2”](#) na página 293

Use uma tarefa de restauração para restaurar dados do EC2 a partir de uma cópia de backup. Por exemplo, se os dados em uma instância forem perdidos ou corrompidos. É possível definir uma tarefa que restaure dados para a zona de disponibilidade original ou para uma zona de disponibilidade diferente na mesma região, com diferentes tipos de opções de recuperação e configurações disponíveis.

[“Iniciando tarefas sob demanda”](#) na página 497

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Restaurando dados do Amazon EC2

Use uma tarefa de restauração para restaurar dados do EC2 a partir de uma cópia de backup. Por exemplo, se os dados em uma instância forem perdidos ou corrompidos. É possível definir uma tarefa que restaure dados para a zona de disponibilidade original ou para uma zona de disponibilidade diferente na mesma região, com diferentes tipos de opções de recuperação e configurações disponíveis.

Antes de Iniciar

Execute as seguintes tarefas:

- Assegure-se de que uma tarefa de backup do EC2 foi executada pelo menos uma vez. Para obter instruções, consulte [“Fazendo backup de dados do Amazon EC2”](#) na página 291.
- Assegure-se de que as funções e os grupos de recursos do IBM Spectrum Protect Plus estejam designados para o usuário que estiver configurando a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 18, “Gerenciando o acesso de”](#), na página 517.

Sobre Esta Tarefa


O IBM Spectrum Protect Plus usa o modo clone para criar cópias de longo prazo de instâncias.

Procedimento

Para definir uma tarefa de restauração do EC2, conclua as etapas a seguir:


1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas Virtualizados > Amazon EC2 > Criar Tarefas**, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Amazon EC2**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
2. Na página **Selecionar origem**, tome as ações a seguir:
 - a) Clique em uma conta na lista para mostrar as instâncias que estão disponíveis para operações de restauração. Também é possível usar a função de procura para procurar por instâncias disponíveis. Insira todo ou parte de um nome para localizar instâncias que correspondam aos critérios de procura. É possível utilizar o caractere curinga (*) para representar todo ou parte de um nome. Use o filtro **Visualização** para alternar as instâncias exibidas.
 - b) Clique no ícone de mais  ao lado da instância que você deseja usar como a origem da operação de restauração.

É possível selecionar mais de uma instância da lista. No entanto, todas as instâncias selecionadas devem estar na mesma região.

Se a instância tiver volumes anexados, será possível navegar nos volumes e selecioná-los para a operação de restauração. Não é possível selecionar ambas as instâncias e os volumes conectados.

As instâncias selecionadas ou os volumes conectados são incluídos na lista de restauração próxima à lista de contas. Para remover um item da lista, clique no ícone de menos  próximo ao item.
 - c) Clique em **Avançar** para continuar.
 3. Preencha os campos na página **Captura Instantânea de Origem** para selecionar as capturas instantâneas de instância que você deseja restaurar e clique em **Avançar** para continuar.

Os campos mostrados dependem do número de instâncias que foram selecionadas na página **Selecionar origem**.

 - Se uma única instância for selecionada, selecione o intervalo de data para as capturas instantâneas que você deseja restaurar. As capturas instantâneas que estão disponíveis para esse intervalo de data são listadas. Selecione a captura instantânea que você deseja restaurar.
 - Se várias instâncias forem selecionadas, selecione o intervalo de data para as capturas instantâneas que você deseja restaurar. As instâncias que possuem capturas instantâneas dentro desse intervalo de data são listadas. Para cada instância, selecione o ponto de restauração que deseja restaurar.
 4. Na página **Configurar Destino**, especifique a Zona de Disponibilidade para a qual você deseja restaurar instâncias e clique em **Avançar**:

Zona de Disponibilidade Original

Selecione esta opção para restaurar instâncias para a Zona de Disponibilidade original.

Zona De Disponibilidade Alternativa

Selecione esta opção para restaurar instâncias para uma Zona de Disponibilidade que seja diferente da Zona de Disponibilidade original e, em seguida, selecione o local alternativo a partir dos recursos disponíveis.

Se você estiver restaurando um volume conectado, selecione a instância de destino na Zona de Disponibilidade alternativa e insira um nome de dispositivo opcional na seção **Anexo de Destino**.

5. Na página **Configurar Rede**, altere a sub-rede para cada Zona de Disponibilidade se você tiver selecionado **Zona de Disponibilidade Alternativa** na página **Configurar Destino**. Se você selecionou **Zona de Disponibilidade Original**, nenhuma configuração será fornecida nesta página. Clique em **Avançar** para continuar.

A sub-rede da Zona de Disponibilidade deve estar na mesma região que as instâncias que são selecionadas na etapa “2” na página 294.

6. Na página **Método de Restauração**, é possível alterar o nome da instância restaurada, inserindo o novo nome da instância no campo **Renomear Instância (opcional)**. Clique em **Avançar** para continuar.
7. Se você estiver executando a tarefa de restauração no modo avançado, será possível configurar opções adicionais como segue:

Inicialização após a recuperação

Alterne o estado de energia de uma instância após uma recuperação ser executada. As instâncias são ligadas na ordem em que são recuperadas.

Continuar com a restauração mesmo que ela falhe

Alterne a recuperação de uma instância em uma série se a recuperação da instância anterior falhar. Se desativada, a tarefa de restauração será interrompida se a recuperação de uma instância 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 instância falhar.

Restaurar tags de instância

Ative esta opção para restaurar tags que são aplicadas em instâncias através do vSphere.

Pré-anexar prefixo ao nome da instância


Insira um prefixo para incluir nos nomes de instâncias restauradas.

Anexar sufixo ao nome da instância

Insira um sufixo para incluir nos nomes de instâncias restauradas.

8. 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.
9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

Resultados

Isso começa depois que você clica em **Enviar** e um registro **onDemandRestore** é incluído na área de janela **Sessões de Tarefas** em seguida. 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  .

Todas as tarefas em execução são visualizáveis na página **Tarefas e operações > Tarefas em execução**.

Tarefas relacionadas

[“Incluindo uma conta do Amazon EC2” na página 290](#)

Quando uma conta do Amazon EC2 é incluída no IBM Spectrum Protect Plus, um inventário das instâncias que estão associadas à conta é capturado. Em seguida, é possível executar tarefas de backup e de restauração e gerar relatórios para as instâncias.

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 43](#).
- 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 *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 por meio dos pontos de restauração que foram copiados 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 `xfsprogs` estiver entre 3.2.0 e 4.1.9, a restauração de arquivo pode falhar devido a um problema conhecido em `xfsprogs` que causa dano em um clone ou sistema de arquivos de captura instantânea quando seu UUID é modificado. Para resolver esse problema, atualize `xfsprogs` para a versão `version 4.2.0` ou posterior. 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 551.

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.

Nota: Somente os objetos de arquivo para os quais uma captura instantânea foi tirada durante o intervalo de data que é especificado serão visíveis. Para esses objetos, quando a seta é clicada ao lado do objeto de arquivo, todas as capturas instantâneas anteriores para esse objeto de arquivo são exibidas.

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 253

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 264

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 11. Protegendo sistemas de arquivos

Os sistemas de arquivos que contêm diretórios e arquivos que você deseja proteger podem ser registrados com IBM Spectrum Protect Plus. Selecione os servidores sistema de arquivos e as unidades que contêm dados que você deseja proteger. Os sistemas de arquivos Microsoft Windows ReFS e NTFS podem ser registrados com IBM Spectrum Protect Plus para que você possa configurar tarefas de backup ou políticas de acordo de nível de serviço (SLA) planejadas regularmente.

É possível proteger sistemas de arquivos locais que são designados a uma letra de unidade. Os volumes em cluster e as ações da unidade não são protegidos pelo IBM Spectrum Protect Plus.

Windows sistemas de arquivos

Depois de registrar com sucesso a máquina que hospeda o Microsoft Windows NTFS ou o ReFS sistema de arquivos com IBM Spectrum Protect Plus, é possível começar a proteger seus dados nos volumes e unidades listados. Você também pode criar um backup on demand de seus dados de sistemas de arquivos ou configurar políticas de acordo de nível de serviço (SLA) para executar tarefas de backup planejadas regulares.

Assegure-se de que seu ambiente no qual o sistema de arquivos está localizado atenda aos requisitos mínimos do sistema. Para obter informações adicionais sobre os requisitos do sistema, consulte [“Requisitos do Sistema de arquivos” na página 50](#).

O endereço IP da máquina que você registra deve ser alcançável a partir do servidor IBM Spectrum Protect Plus e do servidor vSnap. Ambos devem ter um serviço Windows Remote Management que esteja atendendo na porta 5985.

O nome completo do domínio deve ser resolvível e roteável a partir do servidor do dispositivo IBM Spectrum Protect Plus e do servidor vSnap.

Pré-requisitos para o sistemas de arquivos

Todos os pré-requisitos para usar o IBM Spectrum Protect Plus com o sistemas de arquivos devem ser atendidos antes de iniciar a proteção de seus recursos.

Os requisitos para trabalhar com sistemas de arquivos com IBM Spectrum Protect Plus estão disponíveis aqui, [“Requisitos do Sistema de arquivos” na página 50](#).

Nota: O ID do usuário para registrar servidores de arquivos do Windows pode ser configurado com uma das configurações do Windows a seguir:

- A conta do usuário do *Administrador do sistema local* com o componente de segurança do Controle de conta do usuário (UAC) configurado como Desativada. Com este usuário, deve-se abrir o sistema Windows **Painel de controle > Configurações de controle de conta do usuário** e mover a régua de controle para **Nunca notificar**.
- Um usuário que é membro do Grupo de administradores locais com a configuração de política de segurança do Modo de aprovação do administrador desativada. Com este usuário, deve-se abrir o sistema Windows **Política de segurança local**. No menu **Configurações de segurança**, escolha **Políticas locais > Opções de segurança > Controle de conta do usuário: Executar todos os administradores na política de Modo de aprovação do administrador** e configure esta opção como Desativada. Assegure-se de que o seu Grupo de administradores locais inclua a opção de política Efetuar logon como serviço.

Pré-requisitos de espaço

Certifique-se de ter espaço suficiente na máquina que hospeda o sistema de arquivos que você está protegendo. Para obter mais informações sobre os requisitos de espaço, consulte [“Requisitos de espaço](#)

para proteção de sistemas de arquivos” na página 300. Quando você estiver restaurando dados para um local alternativo, deixe um espaço extra. Nenhum arquivo é sobrescrito durante o processo de restauração. Quando os arquivos de nomes idênticos forem localizados, ambas as cópias serão retidas.

Manipulando um certificado de segurança para Windows

Para garantir o acesso para proteção de arquivos do sistema de arquivos com o IBM Spectrum Protect Plus, deve-se criar um certificado e gerenciar sua colocação.

Sobre Esta Tarefa

Nota: Se o serviço de restauração não puder carregar o certificado, os arquivos serão excluídos e um novo certificado autoassinado e chave são criados.

Dica: Se o agente de sistemas de arquivos IBM Spectrum Protect Plus tiver sido executado, você encontrará um certificado autoassinado e chave no local a seguir: %LOCALAPPDATA%\FSPA\. Se o agente ainda não tiver sido executado, siga as etapas para criar e mover o certificado autoassinado e a chave.

O administrador pode acessar esse diretório no seguinte caminho: C:\Users\Administrator\AppData\Local\

Procedimento

1. Crie uma chave e um certificado assinado para a máquina do cliente.
Nem a chave nem o certificado pode ter uma proteção por senha, pois isso afeta o carregamento de arquivos.
2. Crie uma pasta de diretórios chamada FSPA em um local como este %LOCALAPPDATA%\FSPA.
3. Copie a chave e o certificado e coloque-os na pasta FSPA.
4. Copie a chave e o certificado nesta pasta.
5. Renomeie a chave para localfspagent.key.
6. Renomeie o certificado para localfspagent.crt.

Requisitos de espaço para proteção de sistemas de arquivos

Antes de iniciar o backup de dados que são armazenados no sistema de arquivos registrado, assegure-se de que você tenha espaço livre em disco suficiente nos hosts de origem e destino e no repositório vSnap.

Incluindo um sistema de arquivos

Para iniciar a proteção dos dados em um ReFS ou NTFS sistema de arquivos, deve-se incluir o endereço do host no qual o sistema de arquivos está localizado. É possível repetir o procedimento para incluir cada host que você deseja proteger com o IBM Spectrum Protect Plus.

Antes de Iniciar

Nota: O ID do usuário para registrar servidores de arquivos do Windows pode ser configurado com uma das configurações do Windows a seguir:

- A conta do usuário do *Administrador do sistema local* com o componente de segurança do Controle de conta do usuário (UAC) configurado como Desativada. Com este usuário, deve-se abrir o sistema Windows **Painel de controle > Configurações de controle de conta do usuário** e mover a régua de controle para **Nunca notificar**.
- Um usuário que é membro do Grupo de administradores locais com a configuração de política de segurança do Modo de aprovação do administrador desativada. Com este usuário, deve-se abrir o sistema Windows **Política de segurança local**. No menu **Configurações de segurança**, escolha **Políticas locais > Opções de segurança > Controle de conta do usuário: Executar todos os administradores na política de Modo de aprovação do administrador** e configure esta opção como Desativada. Assegure-se de que o seu Grupo de administradores locais inclua a opção de política **Efetuar logon como serviço**.

Sobre Esta Tarefa

Para incluir um sistema de arquivos no IBM Spectrum Protect Plus, deve-se ter o nome do DNS ou o endereço IP da máquina, um ID do usuário e a senha.

Procedimento

1. Na navegação, expanda **Gerenciar proteção > Sistemas de Arquivos > Microsoft Windows**.
2. Na página **Microsoft Windows**, clique em **Gerenciar Servidores de Arquivos** e clique em **Incluir Servidor de Arquivos** para incluir o servidor host.

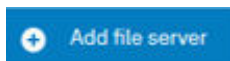


Figura 22. Incluindo um servidor de sistema de arquivos

3. Na seção **Propriedades do Servidor de Arquivos**, insira o nome DNS ou o endereço IP da máquina.
4. Especifique o tipo de usuário para o servidor Windows que você está adicionando.
 - Use um ID de usuário e senha existentes.
 - Insira um novo ID do usuário e senha.

Nota: O ID do usuário para registro de sistemas de arquivos Windows deve ser configurado com uma das seguintes definições do Windows:

- A conta do usuário do Administrador do Sistema Local com o componente de segurança Controle de Conta do Usuário (UAC) desativado. Com esse usuário, deve-se acessar o diálogo Configurações de Controle de Conta do Usuário em seu sistema Windows **Painel de Controle** e mover a régua para **Nunca**.
- Um usuário que é membro do Grupo de administradores locais com a configuração de política de segurança do Modo de aprovação do administrador desativada. Com esse usuário, você deve acessar o diálogo Configurações de Segurança Local em seu sistema Windows e desativar a configuração **Controle de Conta do Usuário: executar todos os administradores na política de Modo de Aprovação Admin**. Assegure-se de que o seu Grupo de administradores locais inclua a opção de política **Efetuar login como serviço**.

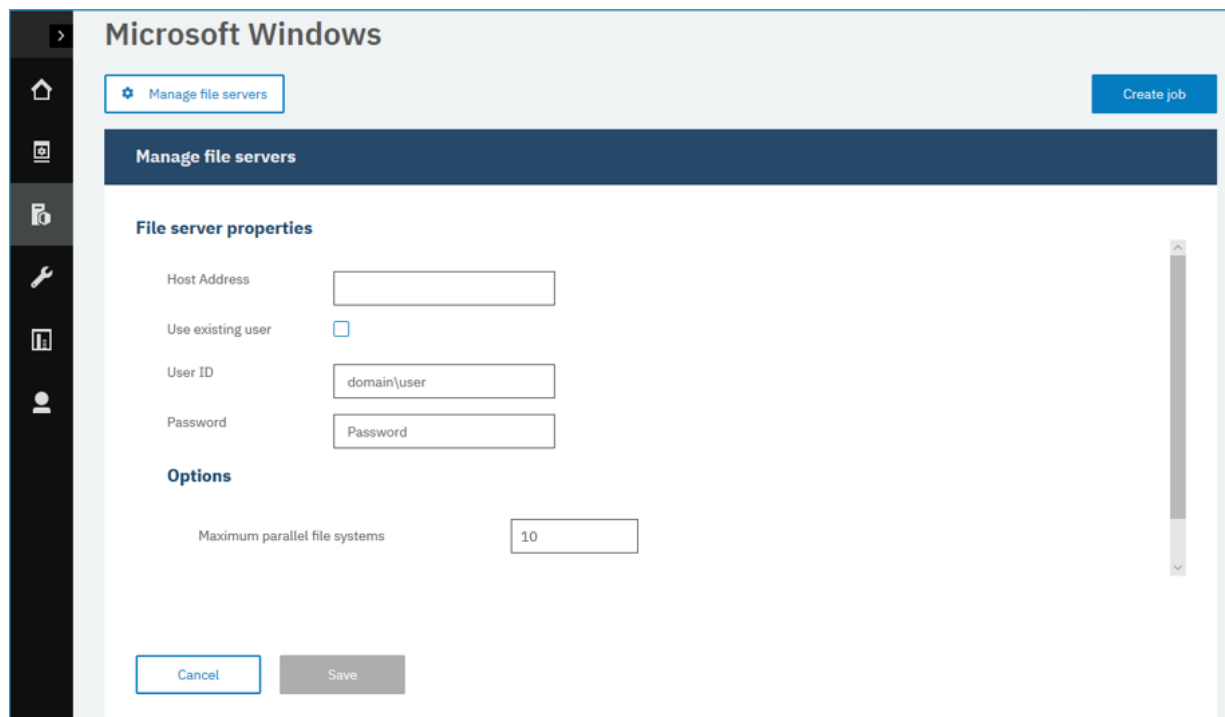


Figura 23. Gerenciando usuários do agente

Importante: Quando você está inserindo o ID do Usuário, não é necessário entrar no domínio.

5. Configure o número máximo de sistemas de arquivos paralelos que devem ser usados para fazer backup de dados do sistema de arquivos que está protegido.

Essa configuração se aplica a cada sistema de arquivos sobre este host. Vários recursos podem ser submetidos a backup em paralelo quando o valor da opção for configurado para mais de 1. Vários sistemas de arquivos paralelos podem acelerar as operações de restauração.

6. Salve o formulário.

O que Fazer Depois

Depois de incluir o host do sistema de arquivos em IBM Spectrum Protect Plus, um inventário é executado automaticamente para detectar os volumes e unidades relevantes.

Para verificar se as unidades e os volumes são incluídos, revise o log da tarefa. Acesse **Tarefas e**



Operações. Clique na guia **Tarefas em Execução** e procure a entrada de log Application Server Inventory que corresponde ao inventário que foi iniciado.

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 sistemas de arquivos devem ser detectados para garantir que eles possam ser protegidos. Para obter instruções sobre como executar um inventário, consulte [Detectando sistemas de arquivos](#).

Executando um inventário para detectar sistemas de arquivos

Depois de incluir um sistema de arquivos no IBM Spectrum Protect Plus, um inventário para detectar volumes, unidades e pontos de montagem é executado automaticamente. O inventário detecta, lista e armazena os recursos do sistema de arquivos que são localizados no host selecionado e disponibiliza os dados para proteção com IBM Spectrum Protect Plus.

Antes de Iniciar

Assegure-se de que você incluiu o sistema de arquivos no IBM Spectrum Protect Plus. Para instruções, consulte [Incluindo um sistema de arquivos](#).

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Sistemas de Arquivos > Microsoft Windows**.

Dica: Para incluir sistemas de arquivos na área de janela **Servidores**, siga as instruções em [Incluindo um sistema de arquivos](#).

2. Clique em **Executar o Inventário**, .

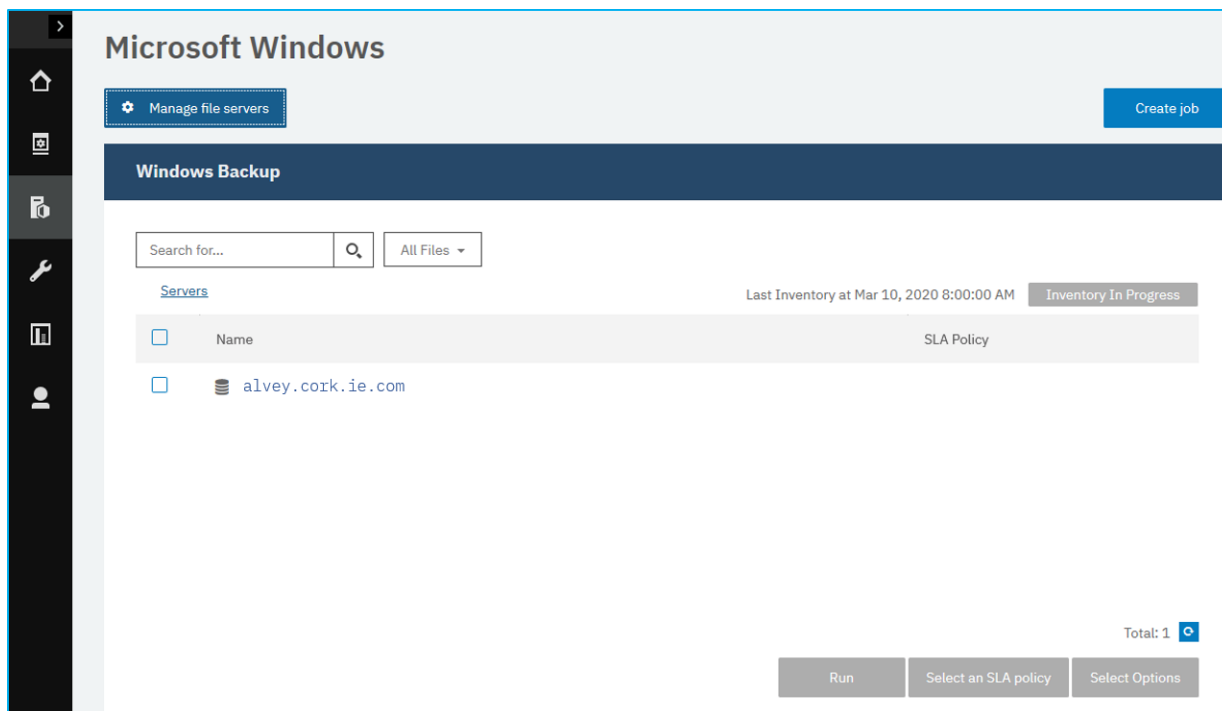



Figura 24. Detectando sistemas de arquivos

Quando o inventário está em execução, o texto muda para mostrar o **Inventário em andamento**. É possível executar um inventário em qualquer servidor sistema de arquivos disponível, mas é possível executar apenas 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 mais nova entrada de log do Application Server Inventory.

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 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. Se a tarefa não for exibida, ajuste o **Período de Histórico da Tarefa** para um intervalo de tempo maior.

3. Clique em um servidor para abrir uma visualização que mostre os volumes, unidades e pontos de montagem que são detectados para aquele servidor. Se alguma entrada estiver ausente na lista **Servidores**, verifique seu sistemas de arquivos e execute novamente o inventário. Em alguns casos, certas entradas são marcadas como ineleáveis para backup; passe o mouse sobre a entrada para revelar o motivo.

Dica: Para retornar à lista de servidores, clique no hipertexto **Servidores**.

Testando a conexão sistemas de arquivos

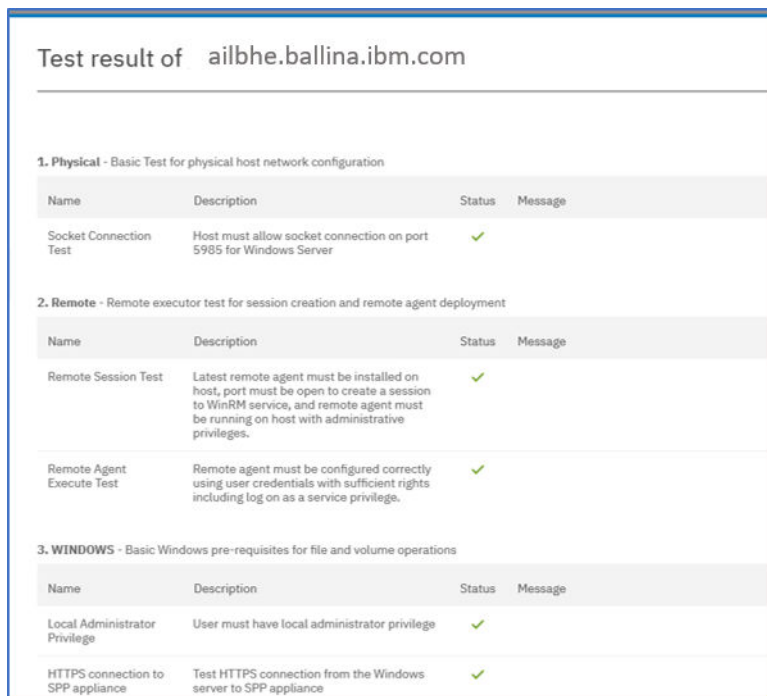
Depois de incluir um sistemas de arquivos, é possível testar a conexão. O teste verifica a comunicação com o servidor e as configurações de DNS entre o IBM Spectrum Protect Plus e o servidor sistemas de arquivos.

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Sistemas de Arquivos > Microsoft Windows**.
2. Na janela **Microsoft Windows**, clique em **Gerenciar Servidores de Arquivos** e selecione o **Endereço de Host** que você deseja testar.

É mostrada uma lista dos hosts da máquina que estão disponíveis.

3. Clique em **Ações** e escolha **Testar** para iniciar os testes de verificação para conexão de rede física, acesso remoto e conexões e configurações de privilégios do Windows.



1. Physical - Basic Test for physical host network configuration			
Name	Description	Status	Message
Socket Connection Test	Host must allow socket connection on port 5985 for Windows Server	✓	
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, port must be open to create a session to WinRM service, and remote agent must be running on host with administrative privileges.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient rights including log on as a service privilege.	✓	
3. WINDOWS - Basic Windows pre-requisites for file and volume operations			
Name	Description	Status	Message
Local Administrator Privilege	User must have local administrator privilege	✓	
HTTPS connection to SPP appliance	Test HTTPS connection from the Windows server to SPP appliance	✓	

Figura 25. Testando a conexão

O relatório de teste mostra uma lista dos testes que foram executados. Ele consiste em um teste para a configuração de rede de host físico, para a instalação do servidor remoto no host e as conexões e privilégios do Windows.

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 sistema de arquivos

Defina as tarefas de backup regulares e especifique opções para executar e criar cópias de backup para proteger os dados do sistema de arquivos.

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 sistema de arquivos IBM Spectrum Protect Plus monta o compartilhamento no servidor 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 sistema de arquivos dos quais deseja fazer backup. Para o procedimento, consulte [Incluindo um servidor sistema de arquivos](#).
- Configure uma Política de Acordo de Nível de Serviço (SLA), conforme descrito nesta tarefa.
- 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 18, “Gerenciando o acesso de”](#), na página 517.
- As tarefas de inventário não devem ser planejadas para serem executadas ao mesmo tempo que as tarefas de backup.

Uma operação de backup falha se o caminho tiver mais de 255 caracteres. Se seus caminhos tiverem mais de 255 caracteres, você deverá ativar caminhos mais longos usando a opção **Ativar Caminhos Longos** do Win32 no editor de políticas do Windows.

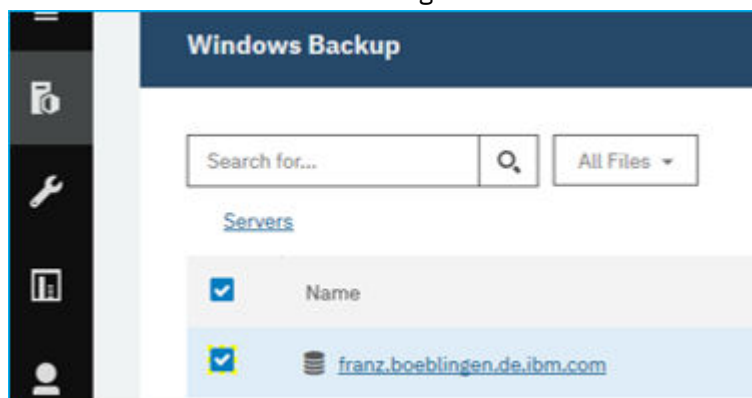
Nota: Nem os compartilhamentos do sistema de arquivos, nem os volumes de cluster da Microsoft podem ser protegidos com IBM Spectrum Protect Plus.

Sobre Esta Tarefa

As etapas a seguir descrevem como fazer backup de recursos que são designados a uma política de SLA. Para executar uma tarefa de backup on demand para um ou mais recursos, independentemente de esses recursos já estarem associados a uma política de SLA, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.

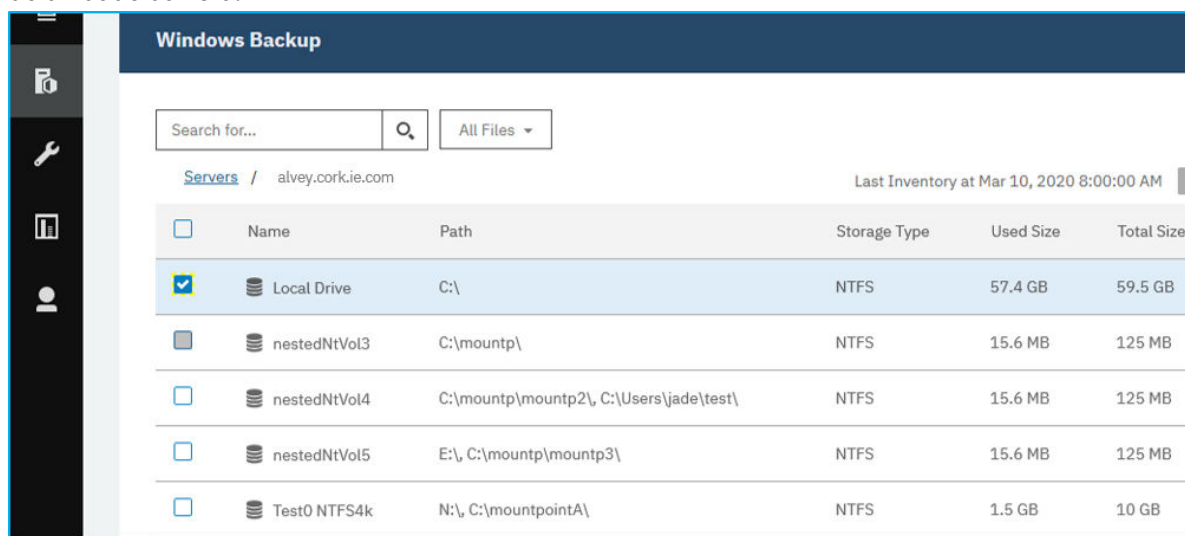
Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Sistemas de Arquivos > Microsoft Windows**.
2. Selecione um servidor do sistema de arquivos para fazer backup na área de janela **Backup do Windows**.
 - Você pode selecionar um servidor sistema de arquivos inteiro clicando na caixa de seleção de nome do servidor. Quaisquer dados incluídos nesse servidor são designados automaticamente à



política de SLA que você escolher.

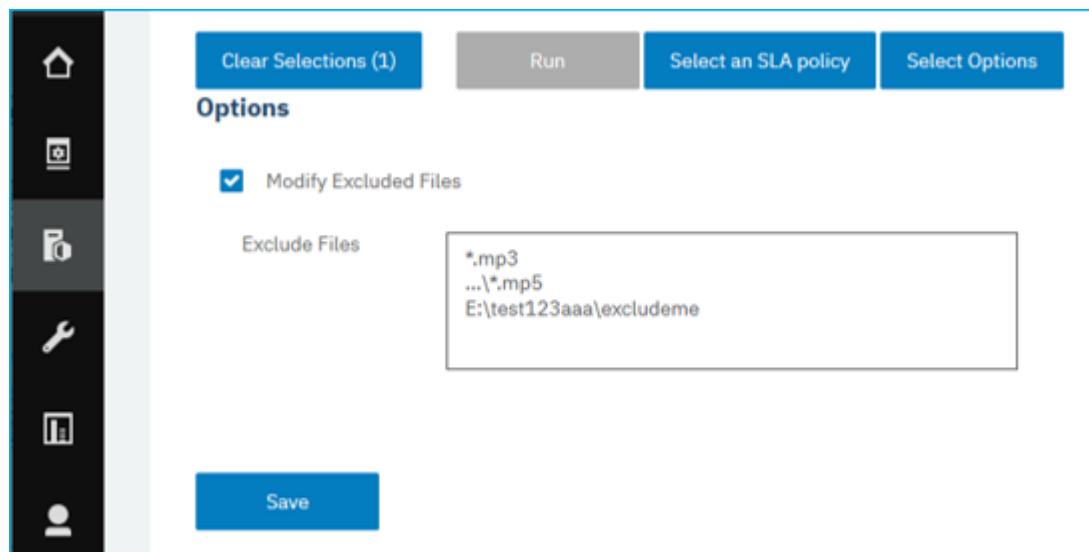
- Ou, você pode selecionar uma unidade ou ponto de montagem específicos de um servidor de sistema de arquivos específico clicando no nome do servidor e escolhendo uma unidade ou ponto de unidade da lista.



3. Clique em **Selecionar Opções** para especificar arquivos a serem excluídos da tarefa de backup que você está configurando. Como alternativa, é possível clicar em **Modificar Arquivos**

Excluídos para deixar as regras de exclusão, pois elas já estão definidas. Clique em **Salvar** para confirmar as mudanças.

Se quiser excluir todos os arquivos de uma unidade, você pode especificar a unidade ou uma pasta em uma unidade como esta Z: \test. Se quiser excluir todos os arquivos de um determinado tipo de sua tarefa de backup, você pode especificar essa exclusão usando uma sequência como este exemplo *.png.

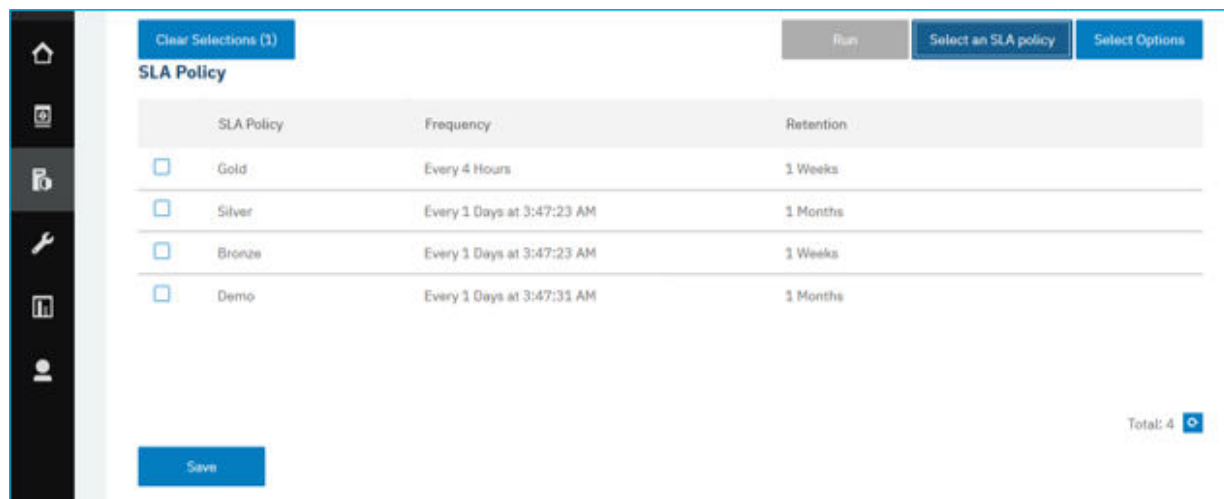


Dica: Para fechar a área de janela **Opções** sem salvar mudanças, clique em **Selecionar Opções**.

4. Selecione o servidor do sistema de arquivos, unidade ou ponto de montagem para backup e clique em

Selecionar uma Política de SLA **Select an SLA policy** para escolher uma política de SLA para esse item.

Você pode escolher entre as opções a seguir: Gold, Silver ou Bronze. Cada tipo de política possui frequências e taxas de retenção diferentes, conforme mostrado na figura a seguir:



SLA Policy	Frequency	Retention
<input type="checkbox"/> Gold	Every 4 Hours	1 Weeks
<input type="checkbox"/> Silver	Every 1 Days at 3:47:23 AM	1 Months
<input type="checkbox"/> Bronze	Every 1 Days at 3:47:23 AM	1 Weeks
<input type="checkbox"/> Demo	Every 1 Days at 3:47:31 AM	1 Months

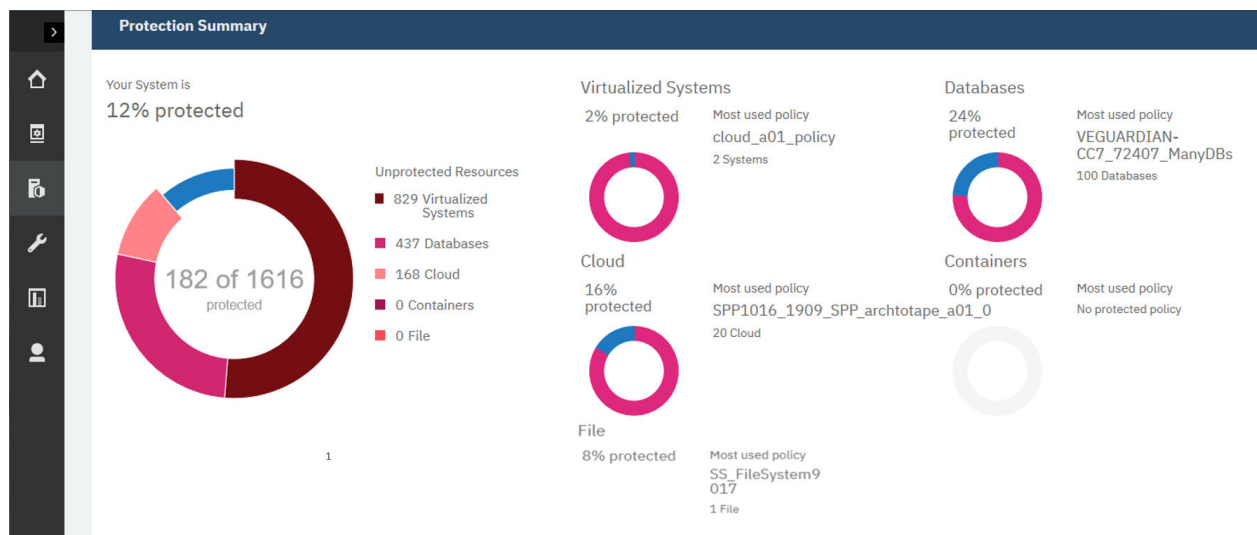
Se você deseja definir uma nova política de SLA, selecione **Gerenciar Proteção > Visão Geral**. Na área de janela **Políticas de SLA**, clique em **Incluir política de SLA** e defina suas preferências de política. Para editar uma política existente com taxas de retenção e frequência customizadas, clique no ícone

de edição  e defina suas preferências. Clique em **Salvar** para confirmar as mudanças.

5. Clique em **Salvar** para salvar a política de SLA.

Se quiser executar a tarefa de backup imediatamente, clique em **Ações > Início**. O status no log muda para mostrar que o backup está Running.

Para visualizar o status de suas políticas de SLA de sistema de arquivos existentes, selecione **Gerenciar Proteção > Visão Geral da Política** para visualizar um resumo de sua proteção, conforme mostrado na figura a seguir:



Quando você está fazendo backup de sistemas de arquivos, é possível definir regras de exclusão para excluir determinadas unidades, diretórios ou arquivos de tarefas de backup. Esses arquivos então não são submetidos a backup como parte de sua política de SLA ou como parte da tarefa de backup ad hoc que você está executando. Quando você executa uma tarefa de restauração, as regras de exclusão significam que as unidades, os diretórios ou os arquivos que são especificados nas regras de exclusão não são restaurados para a nova cópia.

Se quiser excluir um arquivo, você pode especificar o nome do arquivo como este Z:\test\excludedFile.txt. Se quiser excluir todos os arquivos de uma pasta, você pode especificar uma regra como esta Z:\test*. Se quiser excluir uma pasta, você pode especificar uma regra como esta DIR Z:\excludedFolder.

Sintaxe	Comportamento de sintaxe
:\\	<ul style="list-style-type: none"> Indica um sistema de arquivos e unidade do Windows. Deve ser incluído em todas as regras, exceto a regra FS. Uma regra não pode iniciar ou terminar com esta sintaxe. Uma regra deve ser iniciada com uma letra de unidade ou curinga seguido por esta sequência.

Tabela 56. Sintaxe de regras de exclusão para Windows (continuação)

Sintaxe	Comportamento de sintaxe
\	<ul style="list-style-type: none"> Indica o próximo nível de diretório. Uma regra não pode terminar com um caractere de barra invertida \.
\...\	<ul style="list-style-type: none"> Indica que a regra se aplica em todos os diretórios abaixo deste nível. Uma regra não pode iniciar ou terminar com uma sequência \ . . . \ . Essa sequência deve estar após a sequência de especificação da unidade.
*	<ul style="list-style-type: none"> Esta sintaxe é o curinga para qualquer caractere ou para qualquer número de caracteres. Ela também é usada quando nenhum caractere é definido. Uma regra pode iniciar ou terminar com esta sintaxe. Quando usada para indicar uma letra de unidade, esta sintaxe deve ser um caractere alfabético. Este curinga não pode ser um caractere de barra invertida \ .
?	<ul style="list-style-type: none"> Esta sintaxe é usada como um curinga para qualquer caractere apenas para uma ocorrência. Uma regra pode começar e terminar com esta sintaxe. Quando esta sintaxe é usada para indicar uma letra de unidade, ela deve ser um caractere alfabético entre A e Z.
DIR	<ul style="list-style-type: none"> Esta sintaxe indica uma regra de diretórios, mas ela não exclui nenhum arquivo no diretório afetado. Esta sintaxe deve ser uma regra de título seguida de um espaço em branco.
FS	<ul style="list-style-type: none"> Indica que uma unidade de sistema de arquivos completa é excluída da tarefa. Esta sintaxe deve ser seguida por uma letra de unidade que pode ser um caractere único ou um curinga.
Espaços	<ul style="list-style-type: none"> Os espaços são permitidos em nomes de arquivos ou nomes de diretórios. Um espaço em branco não é permitido antes de uma barra invertida, \, ou em um título ou rodapé em uma linha de regra. Os espaços são validados como caracteres únicos.

Tabela 56. Sintaxe de regras de exclusão para Windows (continuação)

Sintaxe	Comportamento de sintaxe
Texto maiúsculo e minúsculo	Microsoft Windows faz distinção entre maiúsculas e minúsculas. As regras de exclusão maiúsculas e minúsculas.

Tabela 57. Instruções de exclusão válidas

Exemplo de regra	
:	Esta regra exclui todos os arquivos da raiz do sistema de arquivos de todas as unidades, mas não exclui os diretórios.
DIR *:*	Esta regra exclui todos os diretórios de todas as unidades, mas não exclui os arquivos no diretório raiz.
DIR E:\...*temp*	Esta regra exclui todos os diretórios cujo nome começa com temp em todos os diretórios da unidade E:.
DIR F:\Users\Bobby*	Esta regra exclui todo o conteúdo do diretório Bobby sem excluir o diretório em si. Os arquivos no diretório Bobby não são excluídos.
DIR F:\Users	Esta regra exclui todos os usuários que estão listados nos diretórios Users e também o diretório Users.
DIR F:\Users\Bobby M?gee	Esta regra exclui todos os diretórios que combinam com o nome com um curinga para uma letra. Essa regra exclui os usuários com nomes como Magee, Megee, Mige e etc.
DIR F:\Users\Bobby Magee	Esta regra exclui o diretório para o usuário que está definido, neste caso Bobby Magee. Com essa regra, o diretório para esse usuário e todo o seu conteúdo que inclui arquivos e subpastas são excluídos.
F:\...*	Esta regra exclui todos os arquivos da unidade F:\, mas não exclui os diretórios.
F:\Bobby.mp?	Esta regra exclui todos os arquivos que correspondem a Bobby .mp? na raiz do sistema de arquivos, como Bobby.MP3, Bobby.MP4, e assim por diante.
F:\Bobby.txt	Esta regra exclui o arquivo Bobby.txt na raiz do sistema de arquivos.
F:\Users\...*.mp3	Esta regra exclui todos os arquivos MP3 para todos os Usuários que estão listados na unidade F.
F:\Users\Bobby\...*.mp3	Esta regra exclui todos os arquivos MP3 do diretório do usuário Bobby.

Tabela 57. Instruções de exclusão válidas (continuação)	
Exemplo de regra	
F:\Users\Bobby\...*music*\...*.mp?	Esta regra exclui todos os arquivos MP em todos os diretórios que possuem a palavra music no nome do diretório para o usuário Bobby. Os arquivos que são excluídos são MP2, MP3, MP4, entre outros.
F:\Users\John* DIR F:\Users\John*	Esta combinação de regra exclui todos os arquivos e todos os subdiretórios para o usuário John, mas não exclui o diretório John em si.
F:\Users\John\tax\Tax_20??.pdf	Esta regra exclui todos os documentos que correspondem ao padrão Tax_20 no diretório John\tax. Arquivos como estes são excluídos: TAX_2000.pdf, TAX_2019.pdf, e assim por diante.
FS F	Esta regra exclui a unidade F do sistema de arquivos.
FS *	Essa regra exclui todas as unidades no sistema de arquivos.
FS ?	Essa regra exclui todas as unidades.

Sintaxe de exclusão inválida

A sintaxe inválida a seguir não funciona em definições de regras de exclusão.

- \no
- *
- *
- F:\no\
- DIR \no
- DIR F:\no\
- DIR *
- DIR F:*\

Para visualizar o arquivo de log da tarefa, acesse **Tarefas e Operações** e abra a guia **Tarefas em Execução**. Localize a entrada de log mais recente do **Application Server Backup**.

Restaurando Dados do sistema de arquivos

Para restaurar dados do sistema de arquivos do repositório do vSnap, defina uma tarefa que restaure dados do backup mais recente ou de uma cópia de backup anterior. Ao usar o navegador File Systems File-Level Restore, é possível selecionar os recursos do sistema de arquivos para incluir na tarefa e especificar se deve-se restaurar dados para a instância original ou para uma instância alternativa em uma máquina diferente.

Antes de Iniciar

Importante: Para todas as operações de restauração, o sistema de arquivos deve estar no mesmo nível de versão nos hosts de origem e de destino. Além disso, deve-se assegurar que uma instância com o mesmo nome que a instância que está sendo restaurada exista em cada host.

Assegure-se de que os seguintes requisitos adicionais sejam atendidos:

- Assegure-se de que pelo menos uma tarefa de backup sistema de arquivos foi executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do sistema de arquivos”](#) na página 304.

- Assegure-se de que as funções e os grupos de recursos do IBM Spectrum Protect Plus estejam designados para o usuário que estiver configurando a tarefa de restauração. Para obter informações adicionais sobre como designar funções, consulte [Capítulo 18, “Gerenciando o acesso de”, na página 517](#).
- Assegure-se de que o destino do IBM Spectrum Protect Plus para sua tarefa de restauração esteja registrado e configurado corretamente.

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. Para obter mais informações sobre os requisitos de espaço, consulte [Requisitos do espaço para proteção do sistema de arquivos](#). Para obter mais informações sobre pré-requisitos e configuração, consulte [Pré-requisitos para proteção do sistema de arquivos](#).

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Sistemas de Arquivos > Microsoft**

Windows e clique em **Criar Tarefa**


Create job

2. Selecione **Restaurar**.

O assistente **Restaurar** é aberto.

3. Opcional: Se você iniciou o assistente de restauração a partir da página **Tarefas e Operações**, clique em **sistema de arquivos** como o tipo de origem e clique em **Avançar**.

Dicas:

- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
4. Na página **Selecionar Origem**, clique em um servidor sistema de arquivos para mostrar os volumes que estão disponíveis nesse servidor. Selecione um volume clicando no ícone de mais ao lado do nome desse volume . Clique em **Avançar** para continuar.
 5. Na página **Captura Instantânea de Origem**, selecione a captura instantânea que você deseja restaurar para o destino. Clique em **Avançar** para continuar.

As capturas instantâneas disponíveis para o volume selecionado são listadas com um registro de data e hora, a política de SLA associada a essa captura instantânea e o tipo de origem que está disponível, seja ele uma cópia de backup, de archive ou de replicação.

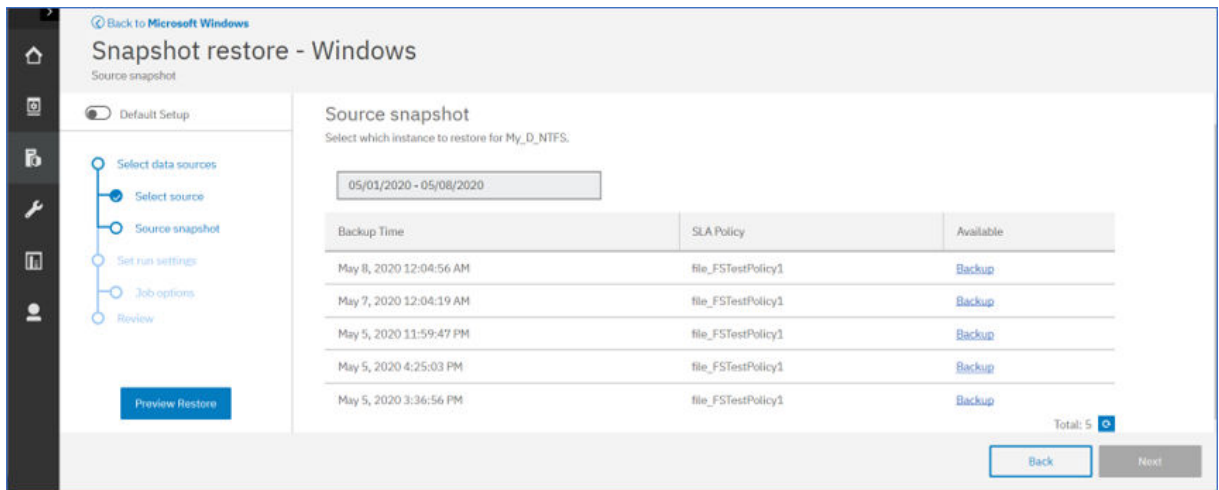


Figura 26. Selecionando captura instantânea de origem

6. Você pode definir as configurações de execução na página **Opções de Tarefa**. Indique se uma operação de limpeza deve ocorrer se a tarefa de restauração falhar. Clique em **Avançar** para continuar.
 7. Na página **Revisar**, revise suas seleções para a tarefa de restauração. Se todas as seleções estiverem corretas, clique em **Enviar** ou clique em **Voltar** para editar as seleções.
- A guia **Recursos Ativos** em Tarefas e Operações é aberta para mostrar o recurso ativo que é preparado quando você sai do assistente de restauração.

Nota: O recurso ativo para a tarefa de restauração que é enviado não é imediato e leva algum tempo para ser exibido.

8. Abra o navegador File Systems File-Level Restore clicando em **Abrir Navegador** na guia **Recursos Ativos**.

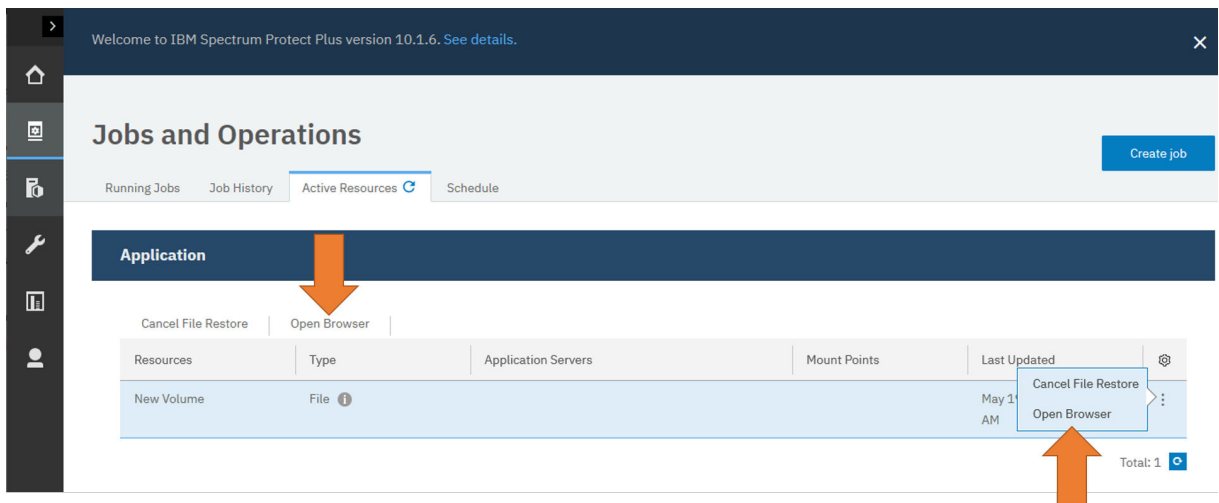


Figura 27. Abrindo o navegador File Systems File-Level Restore a partir da guia Recursos Ativos

9. No navegador **File Systems File-Level Restore**, selecione os recursos do sistema de arquivos para



incluir na tarefa de restauração. Inclua itens clicando no ícone de inclusão ao lado do item apropriado.

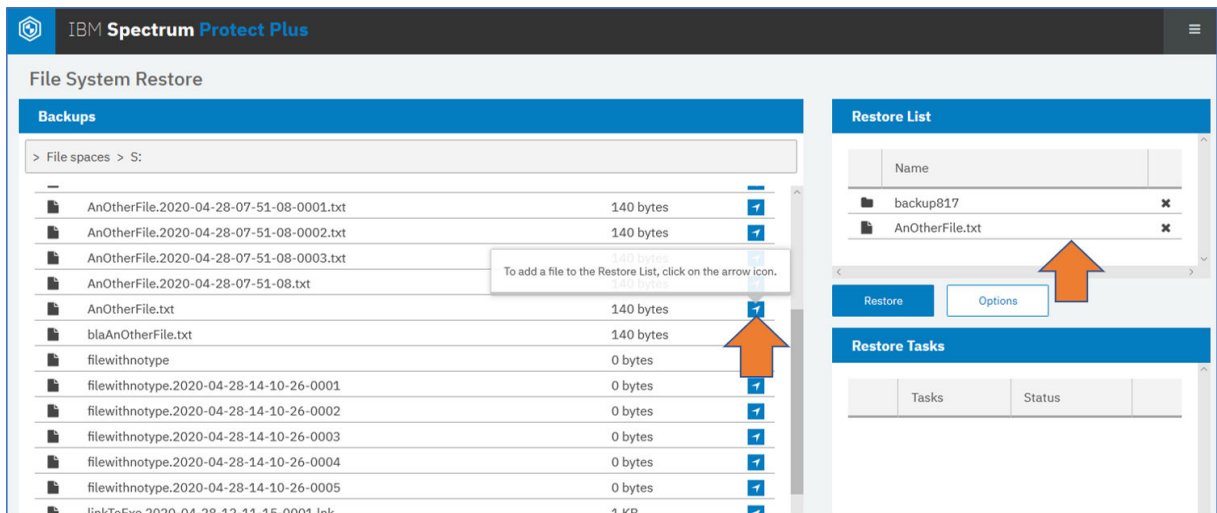


Figura 28. Navegador File Systems File-Level Restore: incluindo recursos na seção Lista de Restaurações

10. Para especificar um local alternativo para a tarefa de restauração, clique **Opções** e digite um caminho de volume local válido do Windows como o destino.

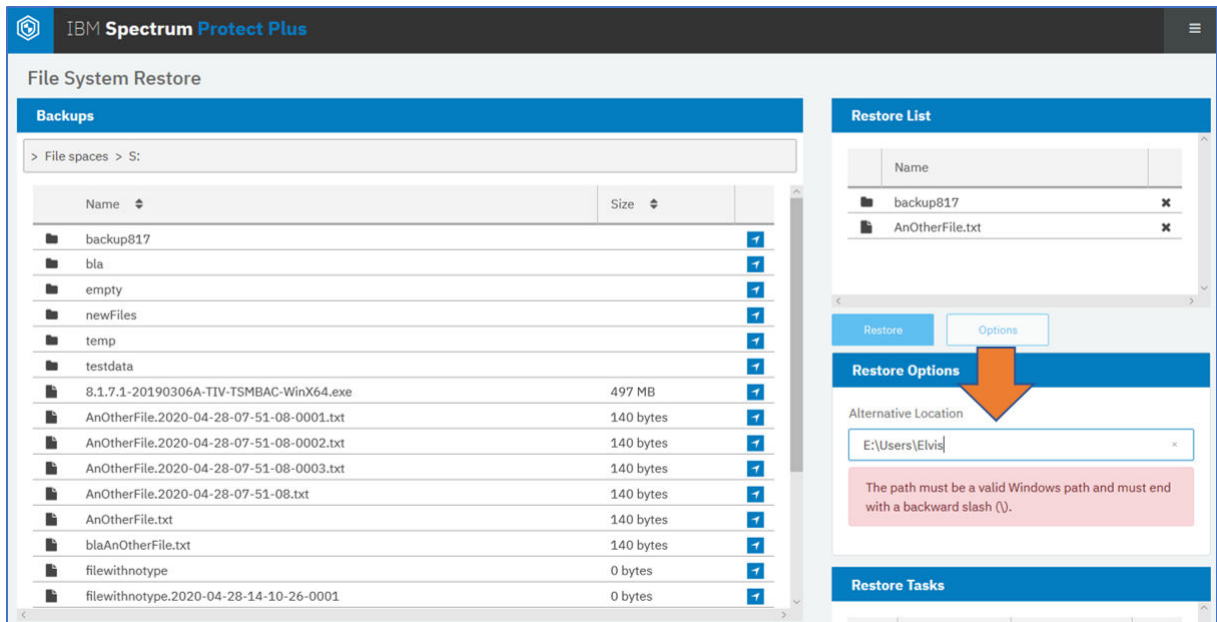


Figura 29. Especificando um local alternativo para a tarefa de restauração no navegador do File Systems File-Level Restore

Restrição: Os compartilhamentos de rede não são locais alternativos válidos para tarefas de restauração.

11. Clique em **Restaurar** para iniciar o processo de restauração.
Nenhum arquivo existente é sobrescrito durante a operação de restauração. Se os arquivos com nomes idênticos forem localizados no destino, um registro de data e hora será incluído no novo arquivo e ambos os arquivos serão armazenados no destino.
12. Opcional: Monitore o progresso da operação de restauração na área de janela **Tarefas de Restauração**.

Dica: O processo de restauração não é rastreado na página IBM Spectrum Protect Plus **Tarefas e Operações**. O progresso da tarefa de restauração é rastreado no navegador File Systems File-Level Restore.

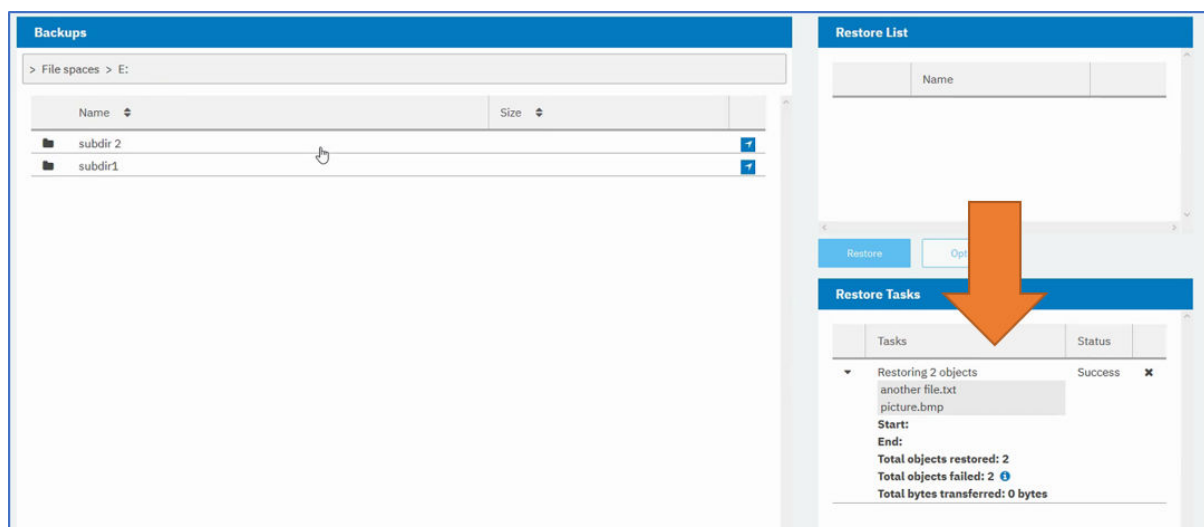


Figura 30. Monitorando a tarefa de restauração no navegador File Systems File-Level Restore

O que Fazer Depois

Quando a tarefa de restauração for concluída, remova o recurso ativo, tomando as seguintes ações:

1. Na área de janela de navegação, clique em **Tarefas e Operações > Recursos Ativos**.
2. Selecione o recurso ativo que você concluiu e clique em **Cancelar Restauração do Sistema de Arquivos**.

Navegador do File Systems File-Level Restore

Ao preparar uma tarefa de restauração para um sistema de arquivos específico, o recurso ativo que é criado pode ser visualizado no navegador **File Systems File-Level Restore** para que você possa definir os itens a serem restaurados. Use o navegador para localizar e especificar os diretórios ou arquivos que você deseja restaurar a partir desse sistema de arquivos. Em seguida, é possível especificar um local alternativo para direcionar os recursos restaurados para um local diferente da origem.

Abrindo o navegador File Systems File-Level Restore

Depois de clicar em **Enviar** no assistente de Restauração, a tarefa de restauração é preparada e a guia **Recursos Ativos** na página **Tarefas e Operações** é aberta. Para abrir o navegador File Systems File-Level

Restore, clique no ícone de ações na tabela **Recursos**



ou clique em **Abrir Navegador** como mostrado.

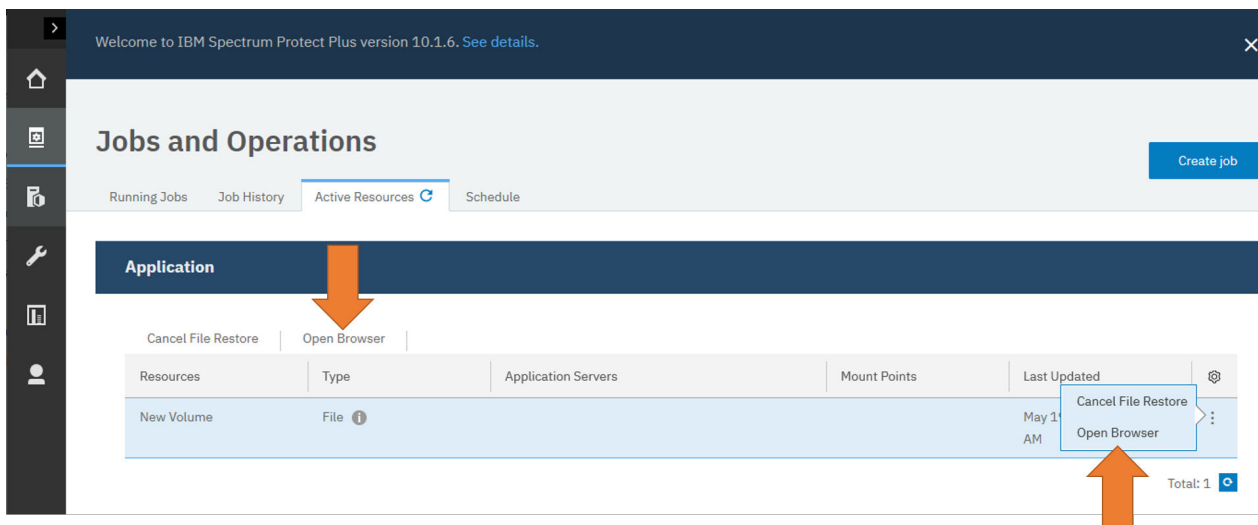


Figura 31. Abrindo o File Systems File-Level Restore a partir da guia Recursos Ativos.

Incluindo recursos na operação de restauração usando o navegador File Systems File-Level Restore

Para incluir recursos do sistema de arquivos específicos em uma tarefa de restauração, navegue até o sistema de arquivos, diretórios ou arquivos necessários. Inclua itens na seção Restaurar Lista clicando no



ícone ao lado do item do sistema de arquivos

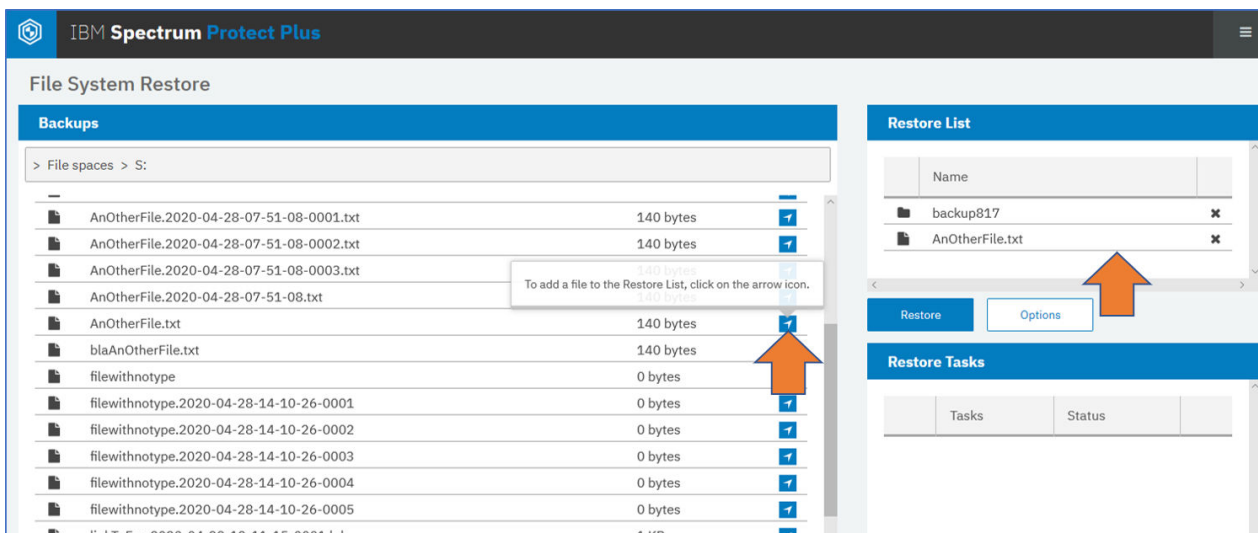


Figura 32. Incluindo objetos do sistema de arquivos para a tarefa de restauração no navegador File Systems File-Level Restore

Restaurando recursos do sistema de arquivos para um local alternativo

Para clonar ou copiar recursos, e restaurar esses recursos para um local diferente do local de origem, é possível especificar um caminho válido do Windows como destino no **Local Alternativo** na área de janela **Opções**.

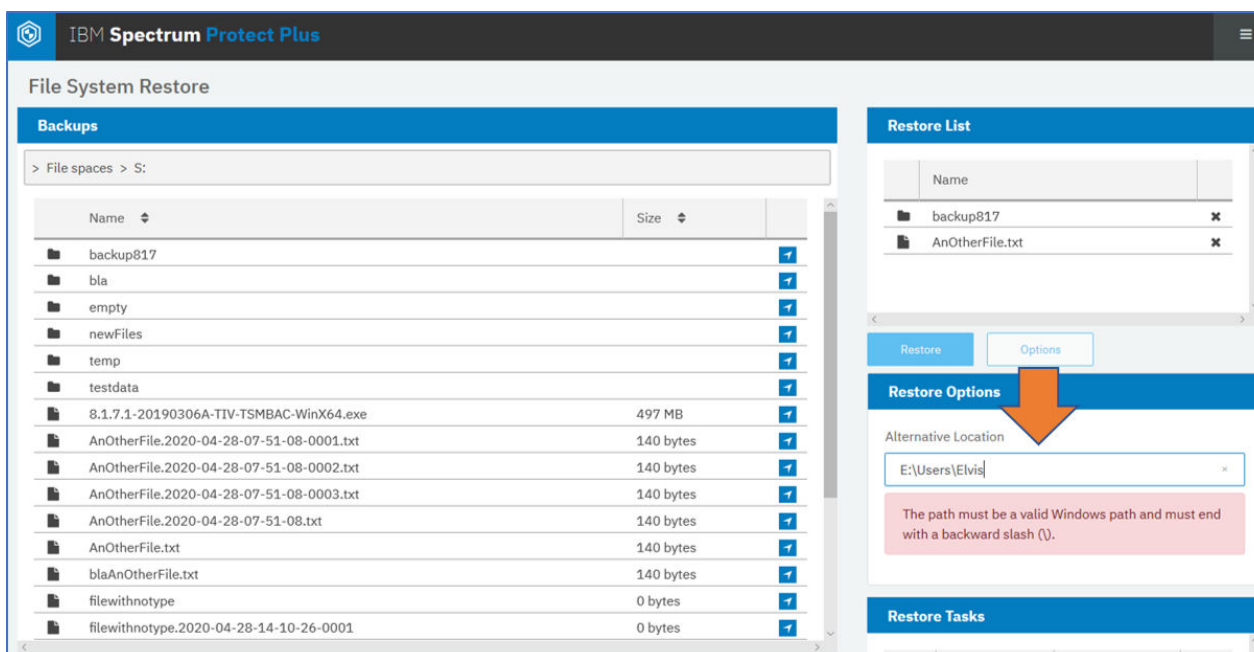
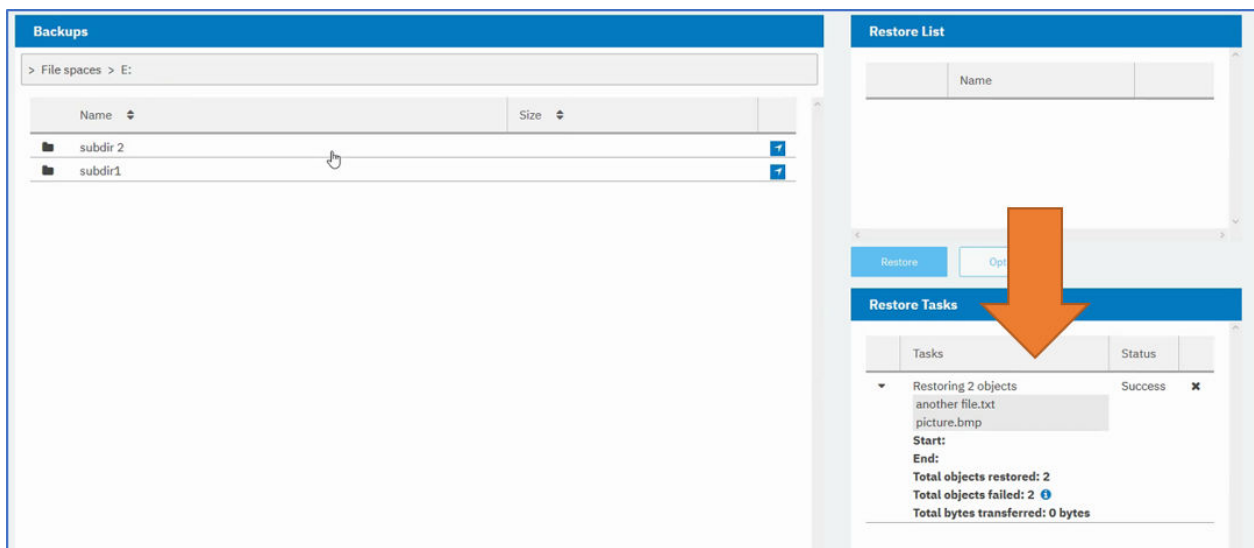


Figura 33. Especificando um local alternativo para a tarefa de restauração no navegador do File Systems File-Level Restore

Monitorando uma tarefa de restauração

Ao clicar em **Restaurar** no navegador File Systems File-Level Restore, é possível monitorar o progresso da tarefa de restauração na área de janela **Restauração de Tarefas**.

Figura 34. Monitorando uma tarefa de restauração no navegador File Systems File-Level Restore



Capítulo 12. Protegendo os contêineres

Suporte de Backup de Kubernetes é um recurso do IBM Spectrum Protect Plus que estende a proteção de dados a contêineres em clusters Kubernetes. Kubernetes é um sistema para orquestrar contêineres através de clusters de hosts.

Para proteger os volumes persistentes no ambiente de Kubernetes, primeiro crie políticas de acordo de nível de serviço que especifiquem a frequência de backup e o período de retenção. Em seguida, crie tarefas para operações de backup e restauração.

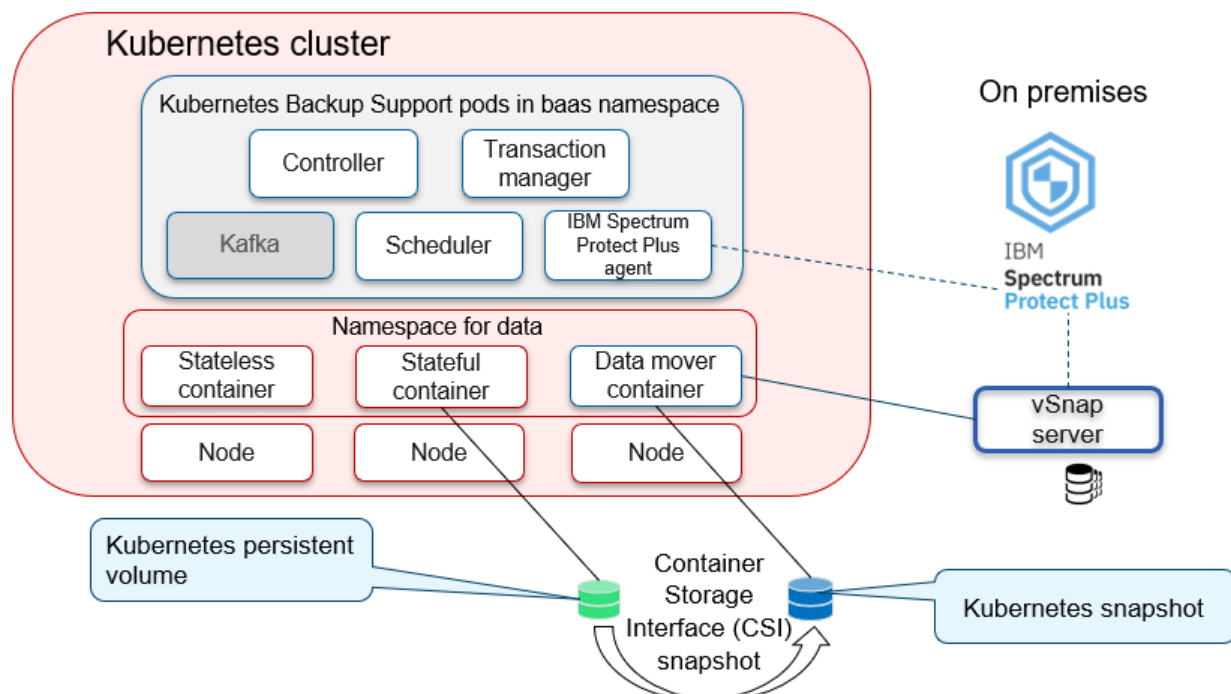
Visão Geral do Suporte de Backup de Kubernetes

Suporte de Backup de Kubernetes do IBM Spectrum Protect Plus protege volumes persistentes que estão conectados a contêineres em Clusters kubernetes. Os backups de captura instantânea dos volumes persistentes são criados e copiados para servidores vSnap IBM Spectrum Protect Plus.

Os volumes persistentes que contêm dados do aplicativo são protegidos por políticas de acordo de nível de serviço (SLA) predefinidas que especificam com que frequência os backups de captura instantânea e de cópia são criados e por quanto tempo eles são retidos. Se os dados nos volumes originais forem danificados ou perdidos, os volumes podem ser restaurados a partir dos backups de captura instantânea ou de cópia nos servidores vSnap.

Suporte de Backup de Kubernetes protege apenas o armazenamento persistente que foi alocado por um plug-in de armazenamento que suporta o Container Storage Interface (CSI) fornecido pelo Kubernetes. O Suporte de Backup de Kubernetes é totalmente testado com o armazenamento de bloco Red Hat Ceph, que suporta CSI. O plug-in do CSI fornece recursos de captura instantânea que são usados para operações de backup.

A figura a seguir mostra como o Suporte de Backup de Kubernetes é implementado no ambiente de Kubernetes e como ele interage com o IBM Spectrum Protect Plus:



Contêiner movedor de dados

O movedor de dados é implementado como um contêiner em um espaço de nomes em que existem solicitação de volume persistente (PVCs). O contêiner do movedor de dados se comunica com a instância do IBM Spectrum Protect Plus fora do ambiente de Kubernetes para o suporte de backup de cópia.

O Suporte de Backup de Kubernetes usa PVCs para identificar os volumes persistentes para backup. Para operações de backup de cópia, quando um planejamento é executado, capturas instantâneas e backups de cópia de um PVC são criados nos intervalos de tempo especificados pelo SLA. O movedor de dados copia os dados e registra os backups de captura instantânea na janela **Tarefas e Operações** do IBM Spectrum Protect Plus. As capturas instantâneas que são criadas por backups on demand também são registradas em IBM Spectrum Protect Plus.

A ocupação variada é suportada

O Suporte de Backup de Kubernetes gerencia operações de backup e restauração usando recursos customizados do Kubernetes. Todos os objetos de backup e restauração pertencem a um espaço de nomes de Kubernetes. O administrador de Kubernetes pode restringir o acesso a esses objetos. Com o acesso controlado, vários usuários podem executar solicitações de backup e restauração no mesmo cluster Kubernetes. Os objetos de backup e restauração herdam um espaço de nomes da PVC que identifica o volume persistente para operações de backup e restauração. Para obter mais informações sobre ocupação variada, consulte [“Recursos de Segurança no Suporte de Backup de Kubernetes” na página 321](#).

Tipos de Backup e Restauração

O Suporte de Backup de Kubernetes fornece vários tipos de funções de backup e restauração. É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou a linha de comandos do Kubernetes para iniciar operações de backup e restauração.

Tipos de Backup

Os seguintes tipos de operações de backup estão disponíveis:

Backup de captura instantânea

Cria um backup do volume persistente usando recursos de captura instantânea de plug-in de armazenamento do Container Storage Interface (CSI). A captura instantânea é armazenada em um local que é designado por uma classe de captura instantânea de Kubernetes, conforme definido pelo administrador de backup. Geralmente, esse local é o mesmo local de armazenamento em que o volume persistente que está submetido a backup. A classe de captura instantânea deve ser compatível com a classe de armazenamento do volume persistente. Em outras palavras, a classe de captura instantânea e a classe de armazenamento são definidas e fornecidas pelo mesmo plug-in de armazenamento CSI.

Os backups de captura instantânea são criados por solicitações de backup planejadas e solicitações de backup on demand.

Durante backups planejados, os backups de captura instantânea são criados em intervalos que são definidos por uma política de acordo de nível de serviço (SLA).

Durante uma solicitação de backup on demand, uma captura instantânea é feita imediatamente, mas nenhum backup de cópia é criado. Após o backup instantâneo inicial, o volume é protegido pela política de SLA especificada.

Backup de cópia

Copia o volume persistente completo para um servidor vSnap do IBM Spectrum Protect Plus. Com base em políticas de SLA predefinidas, o IBM Spectrum Protect Plus oferece retenção mais longa de backups de cópia em comparação com backups de captura instantânea.

Durante os backups planejados, os backups de captura instantânea e de cópia são criados em intervalos definidos pela política de SLA.

Tipos de Restauração

Os seguintes tipos de operações de restauração estão disponíveis:

Restauração de captura instantânea

Restaura uma captura instantânea para um novo volume persistente. Esse tipo de operação é adequado para restaurar rapidamente os backups recentes de captura instantânea.

Restauração de backup de cópia

Restaura um backup de cópia para o volume persistente original ou para um novo volume persistente. Se você deseja restaurar um backup de cópia para o volume persistente original, o contêiner ao qual o volume persistente está conectado não deve estar em execução.

Esse tipo de operação é adequado para restaurar volumes persistentes a partir de backups de cópia que são retidos por um período mais longo no IBM Spectrum Protect Plus.

Políticas de SLA

As políticas de acordo de nível de serviço (SLA) definem com que frequência as operações de backup de captura instantânea e backup de cópia são executadas e por quanto tempo são retidos. Também é possível configurar SLAs customizados que atendem aos seus requisitos operacionais.

O administrador de armazenamento pode criar políticas de SLA usando a interface com o usuário do IBM Spectrum Protect Plus. Para obter instruções, consulte [“Criando uma política de SLA para cluster de Kubernetes” na página 242](#).

Para visualizar a lista de políticas de SLA que são criadas para contêineres, use um dos métodos a seguir:

- Na interface com o usuário do IBM Spectrum Protect Plus, clique em **Gerenciar Proteção > Visão Geral de Política**. A seção **Políticas de SLA** lista todas as políticas que estão disponíveis. Uma política de SLA predefinida, **Contêiner**, está disponível para ajudá-lo a proteger seus volumes persistentes. A política **Contêiner** executa as operações a seguir:
 - Fazer backups de captura instantânea a cada seis horas com um período de retenção de um dia
 - Copiar backups diariamente com um período de retenção de 31 dias
- No ambiente do Kubernetes, emita o seguinte comando para visualizar as políticas de SLA no objeto ConfigMap baas-sla no espaço de nomes baas:

```
kubectl describe configmap baas-sla -n baas
```

Esse comando mostra as políticas de SLA disponíveis para contêineres. Se nenhuma política de SLA foi criada para contêineres, a saída estará vazia.

A saída é semelhante ao seguinte exemplo:

```
Name:          baas-sla
Namesapce:     baas
Labels:        app=baas
               component=scheduler
               release=10.1.6
Annotations:   <none>

Data
====
SLAs:
----
daily_midnight:
Snapshots are performed every 1 days and retained for 7 days.
No copy backups are performed.
----
every_4hours:
Snapshots are performed every 4 hours and retained for 1 days.
No copy backups are performed.
----
hourly:
Snapshots are performed every 1 hours and retained for 1 days.
No copy backups are performed.
```

O SLA é designado a um volume na definição de planejamento de backup. É possível designar mais de um SLA a um volume.

Quando os backups de captura instantânea e de cópia expiram, eles são marcados para expiração no IBM Spectrum Protect Plus e excluídos por tarefas de manutenção do IBM Spectrum Protect Plus.

Tarefas relacionadas

“Definindo backups de acordo de nível de serviço de volumes persistentes” na página 325

É possível usar a interface com o usuário do IBM Spectrum Protect Plus para definir tarefas de backup que são executadas de acordo com uma política de acordo de nível de serviço (SLA). A política de SLA especifica com que frequência as operações de backup são executadas e por quanto tempo os backups de captura instantânea ou de cópia são retidos.

“Planejando backups de volumes persistentes usando a linha de comandos” na página 338

Ao usar a linha de comandos do Kubernetes, é possível planejar solicitações de backup com base em políticas de acordo de nível de serviço (SLA). As políticas de SLA especificam com que frequência as operações de backup são executadas e por quanto tempo os backups de captura instantânea e de cópia são retidos.

Funções de Usuário

Dependendo de sua função, os desenvolvedores de aplicativos corporativos e os administradores de backup interagem com diferentes interfaces com o usuário para proteger dados persistentes em contêineres.

Desenvolvedor de aplicativos

O desenvolvedor de aplicativos corporativos usa a ferramenta de linha de comandos do Kubernetes (**kubect1**) para concluir as seguintes tarefas independentes do administrador de backup:

- Inicia solicitações de backup e restauração de autoatendimento
- Seleciona uma política de acordo de nível de serviço (SLA) para usar em solicitações de backup para proteger seus volumes
- Restaura volumes
- Visualiza o status de solicitações de backup e restauração
- Consulta informações sobre backups de captura instantânea e cópia
- Remove atribuições de política de SLA do PVCs
- Remove solicitações de backup planejado obsoletas e solicitações de captura instantânea on demand

Administrador de Backup

O administrador de backup conclui as seguintes tarefas:

- Implementa e configura o software Suporte de Backup de Kubernetes no ambiente de Kubernetes
- Cria a classe de armazenamento Kubernetes para volumes persistentes e a classe de captura instantânea para armazenar capturas instantâneas
- Instala e configura o IBM Spectrum Protect Plus
- Conclui as tarefas a seguir na interface com o usuário do IBM Spectrum Protect Plus:
 - Registra manualmente um cluster de Kubernetes ou atualiza as propriedades do cluster
 - Executa manualmente um inventário para detectar recursos de cluster
 - Cria políticas de SLA
 - Define tarefas de backup do SLA para proteger volumes
 - Remove atribuições de política de SLA do PVCs
 - Restaura volumes
 - Monitora tarefas de inventário, backup e restauração usando a interface com o usuário do IBM Spectrum Protect Plus

- Gera relatórios que mostram o histórico de tarefas de backup de contêiner usando a interface com o usuário do IBM Spectrum Protect Plus
- Conclui tarefas de resolução de problemas, como coleta de arquivos de log para depuração no ambiente de Kubernetes e visualização de arquivos de log de rastreamento para Suporte de Backup de Kubernetes

Recursos de Segurança no Suporte de Backup de Kubernetes

Além dos recursos básicos de segurança que são integrados ao Suporte de Backup de Kubernetes, os recursos avançados de segurança são fornecidos para ajudar a proteger contêineres, assegurar conexões de rede, criptografar dados e verificar pacotes de instalação.

Varredura de segurança de contêineres

Os componentes do Suporte de Backup de Kubernetes são construídos em contêineres que são derivados da Red Hat Universal Based Image (UBI). O software Suporte de Backup de Kubernetes em cada contêiner foi digitalizado estaticamente para componentes ou bibliotecas vulneráveis. Além disso, os contêineres são digitalizados dinamicamente para ajudar a evitar vulnerabilidades de tempo de execução, como a injeção de código. Após a varredura, o software é testado usando uma suíte de teste automatizada para verificar se o Suporte de Backup de Kubernetes pode operar como esperado e processar corretamente a entrada errônea.

Todos os contêineres, exceto o contêiner movedor de dados, são executados em um espaço de nomes dedicado que proporciona maior isolamento de segurança. O movedor de dados deve ser executado no mesmo espaço de nomes que a solicitação de volume persistente (PVC) para operações de backup ou restauração porque a montagem do volume é limitada a contêineres em um único espaço de nomes.

Contêineres menos privilegiados

Cada um dos componentes em Suporte de Backup de Kubernetes é executado sob o princípio de menor privilégio. As ações dos contêineres são restringidas pelas regras de controle de autenticação baseadas em função que estão associadas a suas contas de serviço em seu espaço de nomes separado. Além disso, o software em cada contêiner é executado como um usuário não raiz. Apenas o movedor de dados é executado como um contêiner privilegiado porque o movedor de dados requer acesso ao ponto de montagem no sistema host do volume que é submetido a backup ou restaurado. Todos os outros contêineres não são privilegiados.

Autenticação de conexões de rede

As conexões de rede entre os componentes do Suporte de Backup de Kubernetes são controladas por políticas de rede que limitam as conexões com aquelas que são necessárias para operação correta. As conexões com IBM Spectrum Protect Plus contam com os protocolos de segurança que são fornecidos pelo IBM Spectrum Protect Plus.

Ocupação Variada

A ocupação variada é suportada no Suporte de Backup de Kubernetes, que depende extensivamente da autenticação e autorização fornecidas pelo cluster de Kubernetes para espaços de nomes. Como a autorização está relacionada a um espaço de nomes, qualquer usuário autorizado a criar um objeto BaaSReq nesse espaço de nomes pode solicitar um backup ou restauração para qualquer PVC que esteja associada a esse espaço de nomes. Um objeto do BaaSReq é um recurso de Kubernetes customizado que é usado em solicitações do Suporte de Backup de Kubernetes.

As capturas instantâneas são protegidas pelo Container Storage Interface (CSI) para restringir o acesso ao espaço de nomes da PVC original. Suporte de Backup de Kubernetes associa o espaço de nomes com as cópias de backup que são armazenadas no IBM Spectrum Protect Plus e as cópias de backup devem ser restauradas em volumes no mesmo espaço de nomes.

Criptografia de dados em repouso

Os administradores de cluster e de armazenamento são responsáveis por ativar os mecanismos de proteção de dados em repouso por meio da criptografia. Os dados sensíveis incluem os dados de backup de cópias e segredos do Suporte de Backup de Kubernetes, que consistem em IDs de usuários e senhas que foram especificados durante o processo de instalação. O administrador do cluster pode especificar que os segredos são criptografados quando armazenados no banco de dados do cluster etcd. Para obter mais informações, consulte [Criptografando Dados Secretos Inativos](#).

Suporte de Backup de Kubernetes não implementa criptografia adicional além do que é fornecido pelo cluster. No entanto, o administrador de armazenamento pode implementar um servidor vSnap IBM Spectrum Protect Plus que está ativado para criptografia.

Ao usar a interface com o usuário do IBM Spectrum Protect Plus, o administrador de armazenamento pode definir acordos de nível de serviço (SLAs) que armazenam dados de backup em discos criptografados. Quando são criadas solicitações de backup que especificam SLAs ativados por criptografia, os dados são direcionados para um servidor vSnap para criptografia se o servidor vSnap estiver ativado para a criptografia de dados em repouso.

Assinatura de Código

O administrador do cluster pode verificar se o pacote de instalação do Suporte de Backup de Kubernetes não foi modificado desde que foi gerado pelo IBM. Esse processo é realizado verificando o arquivo de assinatura que está incluído no pacote de instalação com relação à assinatura e aos certificados apropriados. O processo de verificação está descrito na documentação de instalação.

Para obter mais informações, consulte [“Instalando e implementando imagens do Suporte de Backup de Kubernetes no ambiente de Kubernetes”](#) na página 152.

Fazendo backup e restaurando clusters Kubernetes usando a interface com o usuário do IBM Spectrum Protect Plus

Para proteger os volumes persistentes que estão conectados a um cluster de Kubernetes, crie políticas de acordo de nível de serviço (SLA) e crie tarefas para operações de backup e restauração na interface com o usuário do IBM Spectrum Protect Plus.

Assegure-se de que seu ambiente de Kubernetes atenda aos requisitos do sistema em [“Requisitos do Suporte de Backup de Kubernetes”](#) na página 54.

Conceitos relacionados

[“Visão Geral do Suporte de Backup de Kubernetes”](#) na página 317

Suporte de Backup de Kubernetes do IBM Spectrum Protect Plus protege volumes persistentes que estão conectados a contêineres em Clusters Kubernetes. Os backups de captura instantânea dos volumes persistentes são criados e copiados para servidores vSnap IBM Spectrum Protect Plus.

[“Protegendo contêineres usando a linha de comandos”](#) na página 336

Como um desenvolvedor de aplicativos em um ambiente de Kubernetes, é possível usar a interface da linha de comandos para fazer backup e restaurar dados do contêiner e para consultar o status de solicitações do Suporte de Backup de Kubernetes.

Registrando um cluster de Kubernetes

Se necessário, é possível usar a interface com o usuário do IBM Spectrum Protect Plus para registrar manualmente um cluster de Kubernetes ou para modificar as propriedades de um cluster de Kubernetes registrado.

Sobre Esta Tarefa

Depois que o Suporte de Backup de Kubernetes é instalado, o host do aplicativo para o contêiner Suporte de Backup de Kubernetes é registrado automaticamente na inicialização do host do cluster em Kubernetes. Quando um cluster é registrado com IBM Spectrum Protect Plus, um inventário dos recursos

no cluster é capturado automaticamente, permitindo que você conclua tarefas de backup e restauração, bem como executar relatórios.


No entanto, se o registro automático foi malsucedido ou se um cluster registrado teve o registro cancelado acidentalmente, será possível registrar manualmente o cluster usando a interface com o usuário do IBM Spectrum Protect Plus.

Também é possível modificar as propriedades do cluster registrado, como alterar a porta SSH usada para conectar-se ao serviço do agente de contêiner Suporte de Backup de Kubernetes.

Por exemplo, se você usar um balanceador de carga para distribuir a carga de trabalho em seu cluster, será possível editar o balanceador de carga para usar o número da porta para o serviço de contêiner do agente Suporte de Backup de Kubernetes. Em seguida, é possível registrar o balanceador de carga e o número da porta com IBM Spectrum Protect Plus para que você não tenha que configurar o número da porta novamente.

Procedimento

Para registrar manualmente um cluster ou para modificar propriedades do cluster, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Contêineres > Kubernetes**.
2. Na página **Kubernetes**, clique em **Gerenciar Clusters**.
3. Execute uma das seguintes ações:
 - Para registrar manualmente um cluster, clique em **Incluir cluster**.
 - Para atualizar as propriedades do cluster existentes, na lista de endereços do host, clique no ícone editar  para o host de cluster que você deseja atualizar.
4. Atualize os campos na seção **Propriedades do Aplicativo**:

Nome do cluster

O nome do host do cluster ou balanceador de carga para o contêiner Suporte de Backup de Kubernetes. Você pode digitar um nome do host ou um endereço IP.

O nome do cluster deve corresponder ao valor que é usado para o parâmetro **CLUSTER_NAME** no arquivo de configuração `baas_config.cfg`.

Endereço de Host

O endereço do host para o host de cluster ou balanceador de carga. É possível inserir um endereço IP ou um nome de domínio completo.

Número de Porta

A porta SSH para a conexão com o serviço de contêiner do agente Suporte de Backup de Kubernetes.

Por padrão, a porta é designada automaticamente pelo Kubernetes durante a instalação do Suporte de Backup de Kubernetes. Para obter esse número de porta, emita o comando a seguir na linha de comandos **kubectl** :

```
kubectl get service -n baas | grep baas-spp-agent
```

A saída é semelhante ao seguinte exemplo:

baas-spp-agent	NodePort	10.110.235.90	<none>	22:31299/TCP	111m
----------------	----------	---------------	--------	--------------	------

O número da porta é a sequência numérica que segue 22 : . No exemplo, o número da porta é 31299.

Usar usuário existente

Marque esta caixa de seleção para usar um nome de usuário e senha digitados anteriormente para o host de cluster. Selecione um nome de usuário a partir da lista **Selecionar Usuário**.

ID do usuário

Insira o nome de usuário para o host do aplicativo. Este campo não estará disponível se você estiver usando um usuário existente.

Para recuperar o nome de usuário do host do aplicativo a partir do objeto `baas-secret`, emita o seguinte comando para obter e decodificar o nome de usuário do movedor de dados:

```
echo ``kubect1 get secret baas-secret -n baas -o yaml | /bin/grep datamoveruser | cut -d: -f2 | tr -d ' ' | base64 -d``
```

Insira o resultado no campo **ID do Usuário**. Por exemplo, digite `W36KdGtLWXtuN6L`.

As credenciais para o host do aplicativo serão incluídas na lista de usuários existentes.

Senha

Insira a senha para o host do aplicativo. Este campo não estará disponível se você estiver usando um usuário existente.

Para recuperar a senha do host do aplicativo a partir do objeto `baas-secret`, emita o comando a seguir para obter e decodificar a senha do movedor de dados:

```
echo ``kubect1 get secret baas-secret -n baas -o yaml | /bin/grep datamoverpassword | cut -d: -f2 | tr -d ' ' | base64 -d``
```

Insira o resultado no campo **Senha**. Por exemplo, insira `w6EFx36vrdPzm0BC5Rth0S66f23PCznL`.

5. Opcional: Preencha o campo na seção **Opções**:

Máximo de PVCs simultâneas

Configure o número máximo de backups de captura instantânea ou de cópia da PVC para criar simultaneamente. O desempenho do cluster é impactado quando você faz backup de muitas PVCs simultaneamente, já que cada PVC usa vários encadeamentos e consome largura de banda ao copiar dados. Use essa opção para controlar o impacto em recursos de cluster e minimizar o impacto nas operações de produção.

O valor padrão é 10.

6. Clique em **Save**. IBM Spectrum Protect Plus confirma uma conexão de rede, inclui o cluster no banco de dados IBM Spectrum Protect Plus e, em seguida, cataloga os recursos de cluster, incluindo espaços de nomes e PVCs.

Se aparecer uma mensagem indicando que a conexão foi malsucedida, revise suas entradas. Se as suas entradas estiverem corretas e a conexão não for bem-sucedida, entre em contato com um administrador de rede para revisar a conexão.

O que Fazer Depois

Para verificar se os clusters estão atualizados, revise o log da tarefa. Na área de janela de navegação, clique em **Tarefas e operações**. Clique na guia **Executando tarefas** e procure a entrada de log mais recente do Inventário do servidor de aplicativos. É possível especificar um filtro para mostrar apenas as tarefas de inventário, clicando no ícone do filtro, selecionando **Inventário** e clicando em **Aplicar**.

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. Se o status da tarefa de inventário for **Parcial**, clique em **Log de Tarefas** e revise as entradas de log para localizar o erro.

Os clusters devem ser detectados para assegurar que seus recursos possam ser submetidos a backup. É possível executar um inventário manual a qualquer momento para detectar atualizações em recursos de cluster. Para obter instruções sobre como executar um inventário manual, consulte [“Detectando recursos de cluster de Kubernetes”](#) na página 325. Para obter instruções sobre como planejar tarefas de backup do Kubernetes, consulte [“Definindo backups de acordo de nível de serviço de volumes persistentes”](#) na página 325.

Detectando recursos de cluster de Kubernetes

Os recursos de cluster de Kubernetes são detectados automaticamente após o cluster ser incluído no IBM Spectrum Protect Plus. No entanto, é possível executar uma tarefa de inventário para detectar quaisquer mudanças que ocorreram desde que o cluster foi incluído.

Sobre Esta Tarefa

Execute uma tarefa de inventário periodicamente para ajudar a assegurar que todos os recursos de cluster sejam detectados e possam ser submetidos a backup.

Procedimento

Para executar uma tarefa de inventário, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Contêineres > Kubernetes**.
2. Na lista de clusters, selecione um cluster ou clique no link para o cluster para navegar para o recurso desejado.
3. Clique em **Executar Inventário**.

Quando o inventário está em execução, o botão **Executar Inventário** muda para **Inventário em Andamento**. É possível executar um inventário em qualquer cluster disponível, mas é possível executar apenas um processo de inventário por vez.

Se você não selecionar um cluster na lista de clusters e clicar em **Executar o Inventário**, uma tarefa de inventário será iniciada para todos os clusters.

O que Fazer Depois

Para monitorar a tarefa de inventário, na área de janela de navegação, clique em **Tarefas e Operações**. Clique na guia **Executando tarefas** e procure a entrada de log mais recente do Inventário do servidor de aplicativos. É possível especificar um filtro para mostrar apenas as tarefas de inventário, clicando no ícone do filtro, selecionando **Inventário** e clicando em **Aplicar**.

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. Se o status de uma tarefa de inventário for Parcial, clique em **Log de Tarefas** e revise as entradas de log para localizar o erro.

Testando a conexão com um cluster de Kubernetes

Você pode testar a conexão com um cluster de Kubernetes incluído no IBM Spectrum Protect Plus. A função de teste verifica a comunicação com o cluster e testa as configurações do servidor de nomes de domínio (DNS) entre o servidor IBM Spectrum Protect Plus e o cluster.

Procedimento

Para testar a conexão com um cluster, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Contêineres > Kubernetes**.
2. Clique em **Gerenciar Clusters**.
A lista de clusters disponíveis é exibida.
3. Role a lista e localize o cluster que você deseja testar.
4. Clique no menu **Ações** que está associado ao cluster e selecione **Teste**.

O relatório de teste mostra uma lista dos testes que foram executados e o status.

Definindo backups de acordo de nível de serviço de volumes persistentes

É possível usar a interface com o usuário do IBM Spectrum Protect Plus para definir tarefas de backup que são executadas de acordo com uma política de acordo de nível de serviço (SLA). A política de SLA

especifica com que frequência as operações de backup são executadas e por quanto tempo os backups de captura instantânea ou de cópia são retidos.

Antes de Iniciar

Execute as seguintes ações:

- Assegure-se de que as solicitações de volume persistente (PVCs) para os volumes que você deseja proteger estejam formatadas. As solicitações de backup são direcionadas para PVCs. As operações de backup de volumes de bloco brutos não são suportadas.
- Se você não planeja usar a política de SLA padrão para contêineres, assegure-se de configurar uma política de SLA. Para obter instruções, consulte [“Criando uma política de SLA para cluster de Kubernetes”](#) na página 242.
- Assegure-se de que as funções e os grupos de recursos apropriados sejam designados ao usuário que executará a tarefa de backup. 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. Para obter instruções, consulte [Capítulo 18, “Gerenciando o acesso de”](#), na página 517.
- Se um PVC estiver associado a múltiplas políticas de SLA, assegure-se de que as políticas não estejam planejadas para serem executadas simultaneamente. Planeje as políticas de SLA para execução com uma quantidade significativa de tempo entre elas, ou combine-as em uma única política de SLA.




Sobre Esta Tarefa


Para iniciar a proteção de suas PVCs em um planejamento regular, você deve aplicar uma política de SLA em sua PVC. A política de SLA também define os locais de destino de backup para suas PVCs.

Procedimento

Para definir uma tarefa de backup do SLA para uma ou mais PVCs, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Contêineres > Kubernetes**.
2. Na área de janela **Backup do Kubernetes**, selecione as PVCs das quais deseja fazer backup. É possível usar um dos seguintes métodos:

Método	Etapas
Como fazer backup de todas as PVCs em um cluster	Marque a caixa de seleção para um nome de cluster. Um cluster é identificado pelo ícone do cluster  .
Para fazer backup de PVCs que estão associadas a um espaço de nomes	<ol style="list-style-type: none">a. Clique em Visualizar > Espaço de Nomes.b. Clique no nome de um cluster que contém os PVCs dos quais você deseja fazer backup. A lista de espaços de nomes dentro do cluster é exibida. Um espaço de nomes é identificado pelo ícone do espaço de nomes .c. Para fazer backup de todas as PVCs no espaço de nomes, marque a caixa de seleção para o espaço de nomes. Para fazer backup de PVCs individuais, clique no link do espaço de nomes e marque a caixa de seleção para cada PVC de que você deseja fazer backup. Uma PVC é identificada pelo ícone PVC .

Método	Etapas
Para fazer backup de PVCs que estão associadas a um rótulo	<ol style="list-style-type: none"> Clique em Visualizar > Rótulo. Clique no nome de um cluster que contém os PVCs dos quais você deseja fazer backup. A lista de rótulos dentro do cluster é exibida. Um rótulo é mostrado como um par chave-valor e identificado pelo ícone de rótulo . Para fazer backup de todas as PVCs designadas a um rótulo, marque a caixa de seleção para um rótulo. Para fazer backup de PVCs individuais, clique no nome do rótulo e marque a caixa de seleção para cada PVC de que você deseja fazer backup.
Para usar a função de procura para filtrar a lista de PVCs por SLA	<ol style="list-style-type: none"> Digite os critérios de procura no campo Procurar por. É possível inserir todo ou parte do nome de uma PVC. Como alternativa, é possível deixar o campo Procurar por vazio para mostrar todas as PVCs em um SLA. Selecione um item a partir do menu Todas as PVCs para filtrar os resultados que correspondem aos critérios de procura. É possível filtrar os resultados para mostrar todas as PVCs, PVCs que não estão em nenhum SLA e PVCs que estão em um SLA específico. Marque a caixa de seleção para cada PVC de que você deseja fazer backup.

- Clique em **Selecionar uma Política de SLA** e selecione uma ou mais políticas a partir da tabela **Política de SLA**. É possível escolher a política padrão **Contêiner** ou escolher políticas de SLA customizadas que você definiu.

Essa ação designa a política de SLA selecionada para as PVCs selecionadas. Se você designar uma política de SLA no nível de rótulo ou de espaço de nomes, quaisquer novas PVCs criadas com o rótulo ou no espaço de nomes serão automaticamente designadas ao SLA.

- Para criar a definição de tarefa, clique em **Salvar**.

A tarefa é executada conforme definido pelas políticas de SLA selecionadas. Para executar a tarefa imediatamente, clique em **Tarefas e operações > Planejamento**. Selecione a tarefa e clique em **Ações > Iniciar**.

Executando tarefas de backup on demand: Quando a tarefa para a política de SLA selecionada for executada, todas as PVCs que estão associadas a essa política de SLA serão incluídas na operação de backup. Para fazer backup apenas de PVCs selecionadas, é possível executar uma tarefa on demand. Uma tarefa on demand executa uma operação de backup de captura instantânea imediatamente.

- Para executar uma tarefa de backup on demand para uma única PVC, selecione a PVC e clique em **Executar**. Se o recurso não estiver associado a uma política de SLA, o botão **Executar** será desativado.
- Para executar uma tarefa de backup on demand para uma ou mais PVCs, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.

O que Fazer Depois

Se necessário, é possível configurar opções adicionais para o SLA. Para obter instruções, consulte [“Especificando opções de SLA para tarefas de backup do Kubernetes”](#) na página 328

Opcional: descontinuando backups de SLA para uma PVC: Se não quiser que uma PVC participe mais de tarefas de backup do SLA, remova a designação de política de SLA da PVC tomando as seguintes ações:

- Na área de janela **Backup do Kubernetes**, navegue pela tabela de clusters, selecione a PVC para a qual deseja descontinuar as operações de backup e clique em **Selecionar uma Política de SLA**.
- Na tabela **Política de SLA**, identifique as políticas de SLA que são designadas à PVC. As caixas de seleção para os SLAs designados são marcadas.

3. Limpe a caixa de seleção para a política de SLA que você deseja remover.
4. Clique em **Salvar**. A política de SLA não é mais designada à PVC.

Conceitos relacionados

[“Tipos de Backup e Restauração” na página 318](#)

O Suporte de Backup de Kubernetes fornece vários tipos de funções de backup e restauração. É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou a linha de comandos do Kubernetes para iniciar operações de backup e restauração.

[“Políticas de SLA” na página 319](#)


As políticas de acordo de nível de serviço (SLA) definem com que frequência as operações de backup de captura instantânea e backup de cópia são executadas e por quanto tempo são retidos. Também é possível configurar SLAs customizados que atendem aos seus requisitos operacionais.

Especificando opções de SLA para tarefas de backup do Kubernetes

Depois de selecionar um acordo de nível de serviço (SLA) para sua tarefa de backup, é possível configurar mais opções para esse SLA. As opções de SLA adicionais incluem executar scripts, excluir recursos da operação de backup e forçar uma cópia de backup de base completa, se necessário.

Procedimento

1. Na área de janela de navegação, clique em **Gerenciar proteção > Contêineres > Kubernetes**.
2. Na coluna **Opções de Política** da tabela **Status de Política de SLA**, clique no ícone da área de

transferência  para uma política de SLA e configure as seguintes opções:

Pré-Script

Marque esta caixa de seleção para executar um script antes de uma execução de tarefa. As máquinas baseadas em Windows suportam scripts em lote e do PowerShell enquanto as máquinas baseadas em Linux suportam shell scripts. 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, limpe a caixa de seleção **Usar servidor de script** e escolha um servidor de aplicativos na lista **Servidor de aplicativos**.

Os scripts e servidores de script podem ser configurados usando a página **Configuração do sistema > Script**.

Pós-script

Marque esta caixa de seleção para executar um script após a execução de uma tarefa. As máquinas baseadas em Windows suportam scripts em lote e do PowerShell enquanto as máquinas baseadas em Linux suportam shell scripts. 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, limpe a caixa de seleção **Usar servidor de script** e escolha um servidor de aplicativos na lista **Servidor de aplicativos**.

Os scripts e servidores de script podem ser configurados usando a página **Configuração do sistema > Script**.

Continuar job/tarefa no erro de script

Marque esta caixa de seleção para continuar executando a tarefa quando o script que está associado com a tarefa falhar.

Quando essa opção estiver ativada, se um pré-script ou pós-script concluir o processamento com um código de retorno diferente de zero, a operação de backup ou restauração será tentada e o status da tarefa de pré-script ou de pós-script será relatado como COMPLETED.

Quando essa opção é desativada, a tarefa de backup ou restauração não é tentada e o status da tarefa pré-script ou pós-script é relatado como FAILED.

Excluir Recursos

Exclua recursos específicos da tarefa de backup usando um ou mais padrões de exclusão. 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 caracteres especiais a seguir: - _ *

Separe vários filtros com um ponto-e-vírgula.

3. Clique em **Salvar**.

Restaurando dados do contêiner

É possível usar a interface com o usuário do IBM Spectrum Protect Plus para restaurar um volume persistente a partir de uma captura instantânea ou de um backup de cópia. Uma operação de restauração instantânea geralmente é o método mais rápido para restaurar um volume persistente.

Antes de Iniciar

Revise as seguintes restrições:

- Não é possível restaurar um backup de captura instantânea ou de cópia para um espaço de nomes ou cluster diferente.
- Não é possível restaurar um backup de captura instantânea ou de cópia para o volume persistente original. É possível restaurar um backup de captura instantânea ou de cópia apenas para um novo volume persistente. A solicitação de volume persistente (PVC) para o novo volume é criada automaticamente durante a operação de restauração.
- Para assegurar que uma solicitação de restauração funcione corretamente, não exclua manualmente quaisquer capturas instantâneas de volumes que sejam protegidas por Suporte de Backup de Kubernetes.

Sobre Esta Tarefa


Para criar a tarefa de restauração, use o assistente **Restaurar**. É possível criar tarefas on demand que sejam executadas uma vez após a conclusão do assistente.


Procedimento


Para restaurar seus volumes persistentes a partir de backups de cópia ou capturas instantâneas, defina uma tarefa de restauração concluindo as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar proteção > Contêineres > Kubernetes**.
2. Clique em **Criar Tarefa** para ir à página **Criar Tarefa**.
3. Na área de janela **Restaurar**, clique em **Selecionar** para abrir o assistente **Restaurar**.

Dicas:

- Você também pode abrir o assistente **Restaurar** clicando em **Tarefas e Operações > Criar tarefa**. Em seguida, clique em **Selecionar** na área de janela **Restaurar** e clique em **Kubernetes**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançada, configure o modo como **Configuração Avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
4. Na página **Selecionar Origem**, navegue na tabela e selecione a PVC que você deseja restaurar clicando no ícone de mais  para a PVC.

As PVCs selecionadas são exibidas na lista **Item**. Se precisar remover um item da lista, clique no ícone de menos  próximo ao item.

Alternativamente, você pode procurar uma PVC especificando todo ou parte do nome da PVC no campo **Procurar por** e clicar no ícone de procura .

5. Na página **Captura Instantânea de Origem**, use um dos métodos a seguir para selecionar a origem da qual você deseja restaurar:

- Para restaurar uma PVC a partir de uma captura instantânea:
 - a. Clique em **Origem > Da Captura Instantânea**.
 - b. Clique em **Tipo de restauração > On Demand** para executar uma operação de restauração única. A tarefa de restauração iniciará imediatamente após a conclusão do assistente. A opção **Recorrente** não se aplica às operações de restauração do Kubernetes.
 - c. Clique no campo de intervalo de data e especifique um intervalo de datas para mostrar os backups de captura instantânea disponíveis dentro desse intervalo de data.
 - d. Se você estiver restaurando uma única PVC, selecione uma captura instantânea na lista de itens disponíveis. Se você estiver restaurando mais de uma PVC, selecione um ponto de restauração para cada PVC que estiver listada.
 - e. Clique em **Avançar** para continuar.
- Para restaurar uma PVC a partir de um backup de cópia:
 - a. Clique em **Origem > Da Cópia**.
 - b. Clique em **Tipo de restauração > On Demand** para executar uma operação de restauração única. A tarefa de restauração iniciará imediatamente após a conclusão do assistente. A opção **Recorrente** não se aplica às operações de restauração do Kubernetes.
 - c. No menu **Restaurar Tipo de Local**, selecione um tipo de local do qual restaurar dados:
 - Site**
O site no qual os dados foram submetidos a backup. O site é definido na área de janela **Configuração do sistema > Site**.
 - Serviço de nuvem**
O serviço de nuvem no qual os dados foram copiados. O serviço de nuvem é definido em **Configuração do Sistema > Armazenamento de Backup > Armazenamento de Objeto**.
 - Servidor do Repositório**
O servidor do repositório onde os dados foram copiados. O servidor do repositório é definido em **Configuração do Sistema > Armazenamento de Backup > Servidor de Repositório**.
 - Archive de serviço de nuvem**
O serviço de archive de nuvem no qual os dados foram copiados. O serviço de nuvem é definido na área de janela **Configuração do sistema > Armazenamento de backup > Armazenamento de objeto**.
 - Archive do servidor do repositório**
O servidor do repositório no qual os dados foram copiados para fita. O servidor do repositório é definido na área de janela **Configuração do sistema > Armazenamento de backup > Servidor do repositório**.
 - d. No menu **Selecionar um Local**, tome uma das ações a seguir:
 - Se você estiver restaurando dados de um site, selecione um dos locais de restauração a seguir:
 - Demo**
O site de demonstração a partir do qual restaurar backups de cópia.
 - Primário**
O site primário do qual restaurar backups de cópia.
 - Secundário**
O site secundário a partir do qual restaurar backups de cópia.
 - Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu **Selecionar uma localização**.

- e. Clique no campo de intervalo de data e especifique um intervalo de datas para mostrar os backups de cópias disponíveis dentro desse intervalo de data.
- f. Se você estiver restaurando uma única PVC, selecione um backup a partir da lista de itens disponíveis. Se você estiver restaurando mais de uma PVC, selecione um ponto de restauração para cada PVC que estiver listada.
- g. Clique em **Avançar** para continuar.

6. Na página **Método de Restauração**, digite um novo nome para a PVC restaurada.

Para designar a nova PVC, é possível inserir até 221 caracteres para o nome da PVC e um prefixo de 32 caracteres. É possível incluir caracteres alfanuméricos, pontos (.) e hífen (-). O novo nome da PVC não deve conter letras maiúsculas e não deve terminar com um hífen ou um ponto. Por exemplo, `restored-pvc1` é um nome de PVC válido.

A PVC pode ser restaurada apenas no modo de produção para o espaço de nomes original.

Clique em **Avançar** para continuar.

7. Na página **Opções de Tarefa**, configure opções adicionais para a tarefa de restauração:

Executar limpeza imediatamente na falha da tarefa

Se a recuperação da PVC falhar, limpe automaticamente os recursos alocados como parte da tarefa de restauração.

Permitir sobrescrição de sessão

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.

Continue com as restaurações das outras PVCs selecionadas, mesmo que uma falhar

Se uma PVC não for restaurada com sucesso, a tarefa de restauração continuará para todas as outras PVCs que estão sendo restauradas. Se essa opção não estiver ativada, a tarefa de restauração será interrompida quando a recuperação de uma PVC falhar.

Clique em **Avançar** para continuar.

8. Opcional: Se você estiver executando o assistente no modo de configuração avançado, na página **Aplicar Scripts**, especifique scripts a serem executados antes ou depois de uma operação ser executada no nível da tarefa. Os scripts Batch e PowerShell são suportados.

Pré-Script

Marque esta caixa de seleção para escolher um script transferido por upload e um servidor de aplicativo ou de script no qual o pré-script será executado. Para selecionar um servidor de aplicativos no qual o pré-script será executado, limpe 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, limpe 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 esta caixa de seleção para continuar executando a tarefa quando o script que está associado com a 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 restauração será tentada e o status da tarefa de pré-script ou de pós-script será relatado como COMPLETED.

Se você limpar essa caixa de seleção, a operação de restauração não será tentada e o status da tarefa pré-script ou pós-script será relatado como FAILED.

9. Na página **Revisar**, revise suas configurações da tarefa de restauração e clique em **Enviar** para criar a tarefa.

Resultados

Para tarefas on demand, uma tarefa começa depois que você clica em **Enviar** e o registro **onDemandRestore** é incluído na área de janela **Sessões de Tarefa** logo em seguida. Para visualizar o progresso da operação de restauração, expanda a tarefa. Você também pode fazer o download do arquivo de log clicando em **Fazer Download do .zip**.

Todas as tarefas em execução são visualizáveis na página **Tarefas e Operações > Tarefas em Execução**.

O que Fazer Depois

Para verificar se a PVC é restaurada, emita o comando **kubect1** a seguir:

```
kubect1 get pvc restored_pvc -n namespace
```

em que *restored_pvc* especifica o nome da PVC restaurada e *namespace* especifica o espaço de nomes da PVC restaurada.

Expirando sessões de tarefa de Kubernetes

Você pode expirar uma sessão de tarefa de backup do Kubernetes para substituir as configurações de retenção que foram designadas quando um backup de captura instantânea ou cópia foi criado. Quando uma sessão de trabalho estiver expirada, o ponto de restauração (o backup de cópia ou captura instantânea) será removido durante a próxima tarefa de manutenção.


Sobre Esta Tarefa

Conclua esta tarefa se você não deseja aguardar uma sessão de tarefa expirar automaticamente de acordo com a configuração de retenção da política de acordo de nível de serviço designada.

Procedimento

Para expirar uma sessão de tarefa de Kubernetes, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > IBM Spectrum Protect Plus > Retenção de Pontos de Restauração**.
2. Na guia **Sessões de Backup**, procure uma sessão de tarefa ou ponto de restauração. Alternativamente, na guia **Máquinas virtuais / Bancos de dados**, selecione **Aplicativos** e procure uma entrada de catálogo inserindo o nome.

Os nomes podem ser pesquisados inserindo o texto parcial, usando o asterisco (*) como um caractere curinga ou usando o ponto de interrogação (?) para correspondência de padrões. Para obter mais informações sobre como usar a função de procura, consulte [Apêndice A, “Diretrizes de Procura”, na página 551](#).
3. Opcional: Se você estiver procurando na guia **Sessões de Backup**, use filtros para restringir sua procura por backups de cópia ou captura instantânea. Você também pode especificar o intervalo de data quando a tarefa de backup associada foi iniciada.
 - a) No campo **Tipo**, selecione **Aplicativo**.
 - b) No campo **Tipo de Subpolítica**, selecione **Captura Instantânea** para procurar backups de captura instantânea ou selecione **Backup** para procurar backups de cópia.
 - c) Se necessário, clique no campo **Intervalo de Tempo de Backup** e selecione um intervalo de data para procurar.
4. Clique no ícone procurar .
5. Nos resultados da procura, selecione a sessão de tarefas que deseja expirar.
6. Se você estiver na guia **Sessões de Backup**, a partir do menu **Ações**, selecione uma das opções a seguir:
 - Para expirar uma única sessão de tarefa, clique em **Expirar**.

- Para expirar todas as sessões de tarefa não expiradas para a tarefa selecionada, clique em **Expirar Todas as Sessões de Tarefa**.

Se você estiver na guia **Máquinas virtuais / Bancos de dados**, clique no ícone excluir  para o recurso que você deseja expirar.

7. Siga as instruções na janela de confirmação e clique em **OK**.

Tarefas relacionadas

[“Gerenciando IBM Spectrum Protect Plus pontos de restauração” na página 492](#)

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.

Monitorando tarefas do Suporte de Backup de Kubernetes e executando relatórios

Como o administrador de backup, é possível usar a interface com o usuário do IBM Spectrum Protect Plus para monitorar tarefas do Suporte de Backup de Kubernetes e criar relatórios que mostrem o histórico de backup dos contêineres.

Visualizar Logs de Tarefa

É possível usar a janela **Tarefas e Operações** para monitorar tarefas do Suporte de Backup de Kubernetes, revisar o histórico de tarefas e visualizar tarefas planejadas.

Sobre Esta Tarefa

É possível identificar as tarefas nas guias **Tarefas em Execução** e **Histórico de Tarefas** da seguinte forma:

- As tarefas de inventário são identificadas pelo rótulo **Inventário do Servidor de Aplicativos**.
- As tarefas de manutenção são identificadas pelo rótulo **Manutenção**.
- Os nomes de tarefas de backup são identificados pelo rótulo `k8s_sl_name`.

O tipo de tarefa é mostrado no campo **Tipo**. Por exemplo, uma tarefa de backup de captura instantânea é identificada pelo tipo `Type: Backup - Snapshot`. Um backup de cópia é identificado pelo tipo `Type: Backup`.

- Os nomes da tarefa de restauração são identificados pelo rótulo `onDemandRestore_timestamp`. O tipo de tarefa é `Type: Restore`.

Procedimento

1. Na área de janela de navegação IBM Spectrum Protect Plus, clique em **Tarefas e Operações**.
2. Clique na guia apropriada:

- Para mostrar as tarefas de inventário, backup e restauração que estão em execução, clique em **Tarefas em Execução**.
- Para mostrar as tarefas que foram executadas com sucesso, que concluíram o processamento com avisos ou as tarefas que falharam, clique em **Histórico de Tarefas**. É possível fazer download de um log da tarefa na página selecionando a tarefa e clicando em **Download.zip**.

O arquivo transferido por download tem a seguinte convenção de nomenclatura:
`JobLog_job_name_timestamp.zip`

- Para visualizar o status das tarefas planejadas, clique em **Planejar**.
- Para pegar um atalho para criar uma tarefa de backup ad hoc ou uma tarefa de restauração sem ir para a página **Kubernetes** na seção **Gerenciar Proteção**, clique em **Criar Tarefa**.

Conceitos relacionados

[“Criando tarefas e programações de tarefas” na página 496](#)

O método para criação de tarefas e planejamentos de tarefas depende do tipo de tarefa.

Tarefas relacionadas

“Visualizando Tarefas” na página 498

Visualize informações sobre o status de suas tarefas em execução e o status geral das tarefas que são concluídas com sucesso ou com falhas ou avisos.

Criando relatórios de histórico de backup para volumes persistentes

É possível executar um relatório para mostrar o histórico de backup de seus volumes persistentes protegidos. Ao visualizar o histórico de backup, é possível determinar se suas tarefas de backup estão em execução conforme planejado.

Antes de Iniciar



Se você pretende planejar um relatório para execução em horários específicos, assegure-se de configurar um servidor SMTP para notificações por e-mail. Para obter instruções, consulte [“Incluindo um servidor SMTP” na página 208](#).



Sobre Esta Tarefa

Para cada solicitação de volume persistente (PVC), o histórico de backup mostra informações sobre as capturas instantâneas do Container Storage Interface (CSI) que foram criadas no ambiente de Kubernetes e os backups que foram copiados para o servidor vSnap do IBM Spectrum Protect Plus. É possível visualizar informações, como a data e hora da operação de backup, o tamanho do backup e a duração da operação de cópia. A partir desses dados, é possível verificar se os seus backups planejados estão em execução de acordo com a política de acordo de nível de serviço (SLA) que você definiu para a PVC.

Procedimento

1. Na área de janela de navegação IBM Spectrum Protect Plus, clique em **Relatórios e Logs > Relatórios**.
2. Na coluna **Nome (Cargo)**, localize a linha **Histórico de Backup do Volume Persistente do Contêiner** e tome uma das ações a seguir:

Ação	Etapas
Para executar um relatório imediatamente	<ol style="list-style-type: none">a. Clique no ícone Executar Relatório .b. Na janela Executar Relatório, modifique os parâmetros conforme necessário e clique em Executar.
Para planejar um relatório com os parâmetros padrão	<ol style="list-style-type: none">a. Clique no ícone Planejar Relatório com Parâmetros Padrão .b. Na janela Planejar Relatório com Parâmetros Padrão, especifique a frequência, o horário de início e o endereço de e-mail de um destinatário.c. Clique em Planejamento.

Ação	Etapas
Para criar um relatório customizado	<p>a. Clique no ícone Criar Relatório Customizado . A janela Criar Relatório Customizado é exibida.</p> <p>b. Na guia Parâmetros, insira um nome e uma descrição para o relatório customizado e modifique os parâmetros de relatório, conforme necessário. O nome do relatório não deve conter espaços.</p> <p>c. Para planejar o relatório para execução em horários específicos, clique na guia Planejar e selecione Definir Planejamento.</p> <p>d. Especifique a frequência, o horário de início e o endereço de e-mail de um destinatário.</p> <p>e. Clique em Salvar Relatório.</p> <p>O relatório customizado é salvo na guia Relatórios Customizados da janela Relatórios.</p>
Para executar um relatório customizado	<p>a. Clique na guia Relatórios Customizados.</p> <p>b. Identifique o relatório que você deseja executar e clique no ícone Executar Relatório Customizado .</p> <p>c. Na janela Executar Relatório Customizado, clique em Executar.</p>

Resultados

Se você executou o relatório imediatamente, o relatório do histórico de backup será exibido na janela **Histórico de Backup do Volume Persistente do Contêiner**. Para fazer download do relatório, clique em **Download** e selecione um formato de relatório. Para retornar à janela **Relatórios**, clique em **Voltar para Relatórios**.

Se você definiu um planejamento para o relatório, o relatório do histórico de backup será executado no horário planejado e enviado para o destinatário que você especificou.

As descrições dos dados relatados são mostradas na tabela a seguir:

Tabela 58. Detalhes do relatório de histórico de backup	
Coluna	Descrição
Política do SLA	A política de SLA que é usada para proteger uma PVC.
Horário de proteção	A data e a hora em que cada tarefa de backup foi concluída.
Status	O status de cada tarefa de backup. Se uma tarefa de backup falhou, uma possível razão é fornecida.
Backup de captura instantânea?	Uma indicação que mostra se a instância de backup é um backup de captura instantânea. Um visto é exibido na coluna para indicar que a instância é um backup de captura instantânea. Quando um visto é exibido, nenhum dado é mostrado nas colunas Tamanho do Backup e Velocidade do Backup .
Tamanho do Backup	Para backups de cópia, a quantidade de dados que foram submetidos a backup no servidor vSnap. Para backups de captura instantânea que foram criados no ambiente de Kubernetes ou para backups que falharam, nenhum tamanho é mostrado.
Velocidade de backup	A taxa na qual um backup de cópia foi concluído. Para backups de captura instantânea ou backups que falharam, nenhum dado é mostrado.

Conceitos relacionados

“Gerenciando relatórios e logs” na página 507

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.

Protegendo contêineres usando a linha de comandos

Como um desenvolvedor de aplicativos em um ambiente de Kubernetes, é possível usar a interface da linha de comandos para fazer backup e restaurar dados do contêiner e para consultar o status de solicitações do Suporte de Backup de Kubernetes.

Assegure-se de que seu ambiente de Kubernetes atenda aos requisitos do sistema em “Requisitos do Suporte de Backup de Kubernetes” na página 54.

Pedidos do Suporte de Backup de Kubernetes

Para proteger os dados do contêiner, é possível enviar solicitações do Suporte de Backup de Kubernetes usando a interface da linha de comandos do Kubernetes.

Uma solicitação Suporte de Backup de Kubernetes é um recurso customizado de Kubernetes que é do tipo BaaSReq. As solicitações são especificadas em arquivos de configuração *YAML Ain't Markup Language* (YAML). A solicitação é, então, enviada usando a interface da linha de comandos **kubect1**.

Tipos de solicitações no Suporte de Backup de Kubernetes

A tabela a seguir mostra os tipos disponíveis de solicitações do Suporte de Backup de Kubernetes. Os tipos de solicitação são especificados como valores para a chave **requesttype** no arquivo YAML. Links para instruções sobre como criar e enviar as solicitações também são fornecidos.

Tabela 59. Tipos de solicitações do Suporte de Backup de Kubernetes

Tipo de solicitação	Descrição	Instruções
Backup	Planeje uma operação de backup para uma solicitação de volume persistente (PVC) (inclui backups de captura instantânea e cópia)	“Planejando backups de volumes persistentes usando a linha de comandos” na página 338
BackupLabel	Faça backup de todas as PVCs que possuem um rótulo específico	“Fazendo backup de volumes persistentes por rótulo usando a linha de comandos” na página 342
BackupNamespace	Faça backup de todas as PVCs que estão em um espaço de nomes específico	“Fazendo backup de volumes persistentes por espaço de nomes usando a linha de comandos” na página 345
OnDemandBackup	Solicite um backup de captura instantânea imediato de uma PVC	“Fazendo backup de um volume persistente on demand usando a linha de comandos” na página 340
Restaurar	Restaure uma PVC a partir de um backup de captura instantânea ou um backup de cópia	“Restaurando dados do contêiner usando a linha de comandos” na página 348
Destroy	Exclua todos os backups de captura instantânea e de cópia e marque a tarefa planejada como destroyed	“Excluindo backups de contêiner” na página 353

Executando uma solicitação

Para iniciar uma solicitação, crie um arquivo de configuração YAML que especifique o tipo de solicitação e forneça os parâmetros necessários. Em seguida, envie a solicitação executando o comando **kubectl create**.

O arquivo de amostra a seguir (`baas-req.yaml`) mostra o formato geral de um arquivo YAML:

```
#-----  
# Filename: baas-req.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: request_name  
  namespace: namespace  
spec:  
  requesttype: request_type  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name
```

em que:

request_name

Especifica o nome da solicitação. Para solicitações de backup planejadas, o nome da solicitação deve corresponder ao nome da PVC.

namespace

Especifica o espaço de nomes no qual o volume persistente existe. Se você não especificar um espaço de nomes, o espaço de nomes padrão será usado.

request_type

Especifica o tipo de pedido. Para obter a lista de tipos de solicitação disponíveis, consulte [“Tipos de solicitações no Suporte de Backup de Kubernetes”](#) na página 336.

[sla_policy]

Especifica uma ou mais políticas de acordo de nível de serviço (SLA) que você atribui à solicitação. Para obter informações sobre as especificações para a política de SLA, consulte [“Planejando backups de volumes persistentes usando a linha de comandos”](#) na página 338.

snapshot_class_name

Especifica a classe de captura instantânea para o volume. Se você não especificar a classe de captura instantânea, a classe de captura instantânea padrão será usada se o contêiner sidecar `csi-snapshotter` na classe de captura instantânea padrão corresponder ao fornecedor do volume. Caso contrário, a solicitação de backup é inválida.

Para iniciar a solicitação que é especificada no arquivo de amostra `baas-req.yaml`, emita o seguinte comando:

```
kubectl create -f baas-req.yaml
```

Para verificar o status de uma solicitação, utilize um dos seguintes métodos:

- Para listar todas as solicitações do Suporte de Backup de Kubernetes em todos os espaços de nomes que você pode acessar, emita o seguinte comando:

```
kubectl get baasreq --all-namespaces
```

- Para exibir o status de todas as solicitações do Suporte de Backup de Kubernetes em um espaço de nomes especificado, emita o seguinte comando:

```
kubectl describe baasreq -n namespace
```

em que *namespace* é o espaço de nomes do volume persistente.

- Para exibir o status de uma solicitação do Suporte de Backup de Kubernetes específica, emita o comando a seguir:

```
kubectl describe baasreq request_name -n namespace
```

em que *request_name* é o nome da solicitação e *namespace* é o espaço de nomes do volume persistente.

Fazendo backup de dados do contêiner

Para proteger os volumes persistentes que estão conectados a um contêiner, é possível planejar operações de backup para serem executadas conforme especificado por políticas de acordo de nível de serviço (SLA) predefinidas. Você também pode criar capturas instantâneas de volumes persistentes imediatamente executando solicitações de backup on demand.

Planejando backups de volumes persistentes usando a linha de comandos

Ao usar a linha de comandos do Kubernetes, é possível planejar solicitações de backup com base em políticas de acordo de nível de serviço (SLA). As políticas de SLA especificam com que frequência as operações de backup são executadas e por quanto tempo os backups de captura instantânea e de cópia são retidos.

Antes de Iniciar

As solicitações de backup são direcionadas a solicitações de volume persistentes (PVCs) para os volumes que você deseja proteger. Antes de planejar uma tarefa de backup, tome as ações a seguir:

- Assegure-se de que a PVC exista dentro do espaço de nomes especificado.
- Assegure-se de que o PVC esteja formatado. Os PVCs devem ser formatados antes que possam ser submetidos a backup. Para que um PVC seja formatado corretamente, ele deve ser montado e gravado para. As operações de backup de volumes de bloco brutos não são suportadas.
- Determine qual política de SLA atribuir a PVCs. Para obter instruções sobre como visualizar as políticas de SLA disponíveis, consulte [“Políticas de SLA” na página 319](#).

Sobre Esta Tarefa

Quando uma tarefa de backup planejada é executada, um inventário dos recursos do cluster é executado automaticamente e uma captura instantânea do volume persistente é criada na frequência que é definida pelo SLA. Se o SLA especificar uma política de backup de cópia, a captura instantânea do volume será copiada para um servidor vSnap IBM Spectrum Protect Plus.

Todas as tarefas de backup são planejadas, exceto para tarefas de backup on demand. Para planejar tarefas de backup para uma PVC, crie um arquivo de configuração YAML com especificações de tarefas e aplique a solicitação na linha de comandos no Kubernetes ambiente de alta disponibilidade.

É possível especificar uma ou mais políticas de SLA por PVC.

Procedimento

1. Opcional: Exiba uma lista de PVCs em seu espaço de nomes emitindo o seguinte comando:

```
kubectl get pvc -n namespace
```

A partir da lista de PVCs, identifique a PVC da qual você deseja fazer backup.

2. Crie um arquivo YAML que define a solicitação de um backup planejado. O arquivo do YAML deve conter as propriedades a seguir:

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq
```



```
metadata:
  nome: request_name
  namespace: namespace
spec:
  requesttype: Backup
  sla: [sla_policy]
  volumesnapshotclass: snapshot_class_name
```

em que:

filename

Especifica o nome do arquivo de configuração do YAML. O tipo de arquivo é .yaml.

request_name

Especifica o nome da solicitação de backup, que deve corresponder ao nome da PVC para o volume que você deseja fazer backup. Por exemplo, para criar uma solicitação de backup para uma PVC denominada dbvol-01, o nome da solicitação deve ser dbvol-01.

namespace

Especifica o espaço de nomes no qual a PVC existe.

[sla_policy]

Especifica a política de SLA que determina o planejamento para operações de backup. Você pode especificar mais de uma política de SLA usando uma lista separada por vírgula dentro dos colchetes.

Por exemplo, para designar a política daily para um PVC, especifique a instrução a seguir:

```
sla: [diário]
```

Para designar as políticas every4hours, daily_midnight e weekly para a PVC, especifique a instrução a seguir no arquivo YAML:

```
sla: [every4hours,daily_midnight,weekly]
```

Como alternativa, é possível usar o seguinte formato para especificar uma única política de SLA:

```
sla:
- daily
```

Ou use o formato a seguir para especificar várias políticas de SLA:

```
sla:
- every4hours
- daily_midnight
- weekly
```

Assegure-se de usar o caso correto ao especificar o nome da política de SLA. Os nomes da política fazem distinção entre maiúsculas e minúsculas em arquivos do YAML.

Para remover todas as designações de SLA de uma PVC, exclua os nomes de políticas de SLA dentro dos suportes, conforme mostrado na seguinte instrução:

```
sla: []
```

Especificar os suportes vazios é o único método que você pode usar para remover todas as designações de SLA da PVC.

snapshot_class_name

Especifica a classe de captura instantânea para o volume. Se você não especificar a classe de captura instantânea, a classe de captura instantânea padrão será usada se o contêiner sidecar csi-snapshotter na classe de captura instantânea padrão corresponder ao fornecedor do volume. Caso contrário, a solicitação de backup é inválida.

3. Envie a solicitação de backup emitindo o comando a seguir:

```
kubectl create -f filename.yaml
```

em que *filename* é o nome do arquivo de configuração do YAML.

Resultados

Após você enviar a solicitação de backup, a primeira operação de backup planejada será iniciada dentro da janela que é definida pela política do SLA. O horário de início do backup é registrado no status de backup.

O que Fazer Depois

Para visualizar informações sobre a operação de backup, emita o comando **kubect1 describe** usando o nome da solicitação ou o nome da PVC. Para obter instruções, consulte [“Visualizando o status de tarefas de backup e restauração”](#) na página 351.

Modificando parâmetros em um arquivo do YAML:

Depois que as tarefas de backup planejadas foram iniciadas, é possível modificar os parâmetros no arquivo YAML e aplicá-los na mesma PVC, se necessário. Por exemplo:

- Para designar uma política de SLA diferente para a PVC ou remover uma atribuição de SLA, edite os valores no campo **sla** no arquivo YAML. Em seguida, aplique o arquivo do YAML usando a interface da linha de comandos **kubect1**.
- Se você não deseja mais que a PVC participe de quaisquer tarefas de backup planejadas, remova as designações de política do SLA atualizando o campo **sla** no arquivo YAML. Para remover a PVC de todos os SLAs, modifique o campo **sla** da seguinte forma:

```
sla: []
```

Em seguida, aplique o arquivo do YAML usando a interface da linha de comandos **kubect1**.

Conceitos relacionados

[“Tipos de Backup e Restauração”](#) na página 318

O Suporte de Backup de Kubernetes fornece vários tipos de funções de backup e restauração. É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou a linha de comandos do Kubernetes para iniciar operações de backup e restauração.

[“Políticas de SLA”](#) na página 319

As políticas de acordo de nível de serviço (SLA) definem com que frequência as operações de backup de captura instantânea e backup de cópia são executadas e por quanto tempo são retidos. Também é possível configurar SLAs customizados que atendem aos seus requisitos operacionais.

[“Pedidos do Suporte de Backup de Kubernetes”](#) na página 336

Para proteger os dados do contêiner, é possível enviar solicitações do Suporte de Backup de Kubernetes usando a interface da linha de comandos do Kubernetes.

[“Resolução de Problemas do Suporte de Backup de Kubernetes”](#) na página 534

Para ajudar a solucionar problemas com Suporte de Backup de Kubernetes, é possível coletar arquivos de log de depuração e visualizar logs de rastreamento. Também é possível seguir procedimentos para diagnosticar problemas.

Fazendo backup de um volume persistente on demand usando a linha de comandos

Para criar uma captura instantânea imediatamente sem esperar que uma tarefa de backup planejada seja executada, execute uma tarefa de backup on demand na interface da linha de comandos do Kubernetes.

Antes de Iniciar

As solicitações de backup são direcionadas a solicitações de volume persistentes (PVCs) para os volumes que você deseja proteger. Antes de planejar uma tarefa de backup, tome as ações a seguir:

- Assegure-se de que a PVC exista dentro do espaço de nomes especificado.

- Assegure-se de que o PVC esteja formatado. Os PVCs devem ser formatados antes que possam ser submetidos a backup. Para que um PVC seja formatado corretamente, ele deve ser montado e gravado para. As operações de backup de volumes de bloco brutos não são suportadas.
- Determine qual política de SLA atribuir a PVCs. Para obter instruções sobre como visualizar as políticas de SLA disponíveis, consulte [“Políticas de SLA” na página 319](#).

Sobre Esta Tarefa

Durante uma operação de backup on demand, apenas uma captura instantânea é criada. Após a conclusão da operação de backup on demand inicial, o volume será protegido de acordo com a política de SLA especificada.

Ao contrário de uma solicitação de backups planejados, o nome da solicitação on demand deve ser exclusivo. Em outras palavras, o nome da solicitação não deve ser o mesmo que o nome da PVC.

Procedimento

1. Opcional: Exiba uma lista de PVCs em seu espaço de nomes emitindo o seguinte comando:

```
kubectl get pvc -n namespace
```

A partir da lista de PVCs, identifique a PVC da qual você deseja fazer backup.

2. Crie um arquivo YAML que defina a solicitação de uma operação de backup on demand. O arquivo do YAML deve conter as propriedades a seguir:

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
tipo: BaaSReq

metadados:
  name: name_of_request
  namespace: namespace
spec:
  requesttype: OnDemandBackup
  pvcname: pvc_name
  sla: [sla_policy]
  volumesnapshotclass: snapshot_class_name
```

em que:

filename

Especifica o nome do arquivo de configuração do YAML. O tipo de arquivo é .yaml.

name_of_request

Especifica o nome da solicitação de backup on demand. O nome deve ser exclusivo e não deve corresponder ao nome da PVC.

Uma nova solicitação de backup on demand deve ser criada para cada backup on demand subsequente da mesma PVC. Em outras palavras, para criar um segundo backup on demand de uma PVC, crie uma nova solicitação e especifique um nome de solicitação diferente (*name_of_request*) no arquivo YAML.

namespace

Especifica o espaço de nomes no qual o PVC existe.

pvc_name

Especifica o nome da PVC para o volume do qual você deseja fazer backup.

[sla_policy]

Especifica a política de SLA que determina o planejamento para operações de backup. Por exemplo, para designar a política *daily* para um PVC, especifique a instrução a seguir:

```
sla: [diário]
```

Assegure-se de usar o caso correto ao especificar o nome da política de SLA. Os nomes da política fazem distinção entre maiúsculas e minúsculas em arquivos do YAML.

Quaisquer SLAs que não estejam na solicitação de backup planejado correspondente para a PVC serão incluídos na lista de SLAs nessa solicitação.

snapshot_class_name

Especifica a classe de captura instantânea para o volume. Se você não especificar a classe de captura instantânea, a classe de captura instantânea padrão será usada se o contêiner sidecar `csi-snapshotter` na classe de captura instantânea padrão corresponder ao fornecedor do volume. Caso contrário, a solicitação de backup é inválida.

3. Inicie a operação de backup on demand emitindo o comando a seguir:

```
kubectl create -f filename.yaml
```

em que *filename* é o nome do arquivo de configuração do YAML.

Resultados

Para visualizar informações sobre o backup, emita o comando **kubectl describe** usando o nome da solicitação ou o nome da PVC. Para obter instruções, consulte [“Visualizando o status de tarefas de backup e restauração”](#) na página 351.

Conceitos relacionados

[“Tipos de Backup e Restauração”](#) na página 318

O Suporte de Backup de Kubernetes fornece vários tipos de funções de backup e restauração. É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou a linha de comandos do Kubernetes para iniciar operações de backup e restauração.

[“Pedidos do Suporte de Backup de Kubernetes”](#) na página 336

Para proteger os dados do contêiner, é possível enviar solicitações do Suporte de Backup de Kubernetes usando a interface da linha de comandos do Kubernetes.

[“Resolução de Problemas do Suporte de Backup de Kubernetes”](#) na página 534

Para ajudar a solucionar problemas com Suporte de Backup de Kubernetes, é possível coletar arquivos de log de depuração e visualizar logs de rastreamento. Também é possível seguir procedimentos para diagnosticar problemas.

Fazendo backup de volumes persistentes por rótulo usando a linha de comandos

É possível criar solicitações de backup para volumes persistentes especificando rótulos. Rótulos são pares chave-valor que são anexados a objetos, como pods ou PVCs. Ao especificar um ou mais rótulos em uma solicitação de backup, é possível fazer backup de todas as PVCs que estão associadas a esses rótulos.

Antes de Iniciar

As solicitações de backup são direcionadas a solicitações de volume persistentes (PVCs) para os volumes que você deseja proteger. Antes de planejar uma tarefa de backup, tome as ações a seguir:

- Assegure-se de que a PVC exista dentro do espaço de nomes especificado.
- Assegure-se de que o PVC esteja formatado. Os PVCs devem ser formatados antes que possam ser submetidos a backup. Para que um PVC seja formatado corretamente, ele deve ser montado e gravado para. As operações de backup de volumes de bloco brutos não são suportadas.
- Determine qual política de SLA atribuir a PVCs. Para obter instruções sobre como visualizar as políticas de SLA disponíveis, consulte [“Políticas de SLA”](#) na página 319.

Procedimento

1. Opcional: Exiba uma lista de PVCs em um espaço de nomes especificado emitindo o comando a seguir:

```
kubectl get pvc -n namespace --show-labels
```

A partir da lista de PVCs, identifique o rótulo que está conectado às PVCs de que deseja fazer backup.

2. Crie um arquivo YAML que defina a solicitação para a operação de backup por rótulo. O arquivo do YAML deve conter as propriedades a seguir:

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
tipo: BaaSReq  
  
metadados:  
  name: name_of_request  
  namespace: namespace  
spec:  
  requesttype: BackupLabel  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name  
  backuplabels:  
    - label_key: value
```

em que:

filename

Especifica o nome do arquivo de configuração do YAML. O tipo de arquivo é .yaml.

name_of_request

Especifica o nome da solicitação de backup por rótulo. O nome deve ser exclusivo e não deve corresponder ao nome da PVC.

namespace

Especifica o espaço de nomes para a solicitação de backup.

[sla_policy]

Especifica a política de SLA que determina o planejamento para operações de backup. Você pode especificar mais de uma política de SLA usando uma lista separada por vírgula dentro dos colchetes.

Por exemplo, para designar a política `daily` para um PVC, especifique a instrução a seguir:

```
sla: [diário]
```

Para designar as políticas `every4hours`, `daily_midnight` e `weekly` para a PVC, especifique a instrução a seguir no arquivo YAML:

```
sla: [every4hours,daily_midnight,weekly]
```

Como alternativa, é possível usar o seguinte formato para especificar uma única política de SLA:

```
sla:  
- daily
```

Ou use o formato a seguir para especificar várias políticas de SLA:

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

Assegure-se de usar o caso correto ao especificar o nome da política de SLA. Os nomes da política fazem distinção entre maiúsculas e minúsculas em arquivos do YAML.

Para remover todas as designações de SLA de um rótulo, exclua os nomes de políticas de SLA dentro dos colchetes, conforme mostrado na seguinte instrução:

```
sla: []
```

snapshot_class_name

Especifica a classe de captura instantânea para o volume. Se você não especificar a classe de captura instantânea, a classe de captura instantânea padrão será usada se o contêiner sidecar `csi-snapshotter` na classe de captura instantânea padrão corresponder ao fornecedor do volume. Caso contrário, a solicitação de backup é inválida.

label_key: value

Especifica o par chave-valor para o rótulo que está conectado às PVCs de que deseja fazer backup. É possível especificar mais de um rótulo.

Depois de designar uma política de SLA no nível do rótulo, quaisquer novas PVCs que você criar com esse rótulo serão automaticamente designadas ao SLA.

Por exemplo, para fazer backup de todas as PVCs que estão associadas ao rótulo `color: red` e ao rótulo `department: sales`, especifique as instruções a seguir:

```
backuplabels:  
- color: red  
- department: sales
```

Restrições:

- Os rótulos de PVC são pares chave-valor. Quaisquer chaves duplicadas com valores diferentes são sobrescritas pelo último par chave-valor.
- A operação de backup por rótulo aplica-se a todas as PVCs que possuem um rótulo específico em todo o cluster. Se alguma das PVCs que foram submetidas a backup pertencer a um espaço de nomes a que você não tem acesso, não será possível restaurar essas PVCs usando a linha de comandos. No entanto, as PVCs podem ser restauradas usando a interface com o usuário do IBM Spectrum Protect Plus, independentemente do espaço de nomes a que pertencem. Para obter mais informações, consulte [“Restaurando dados do contêiner”](#) na página 329.

3. Envie a solicitação de backup emitindo o comando a seguir:

```
kubectl create -f filename.yaml
```

em que *filename* é o nome do arquivo de configuração do YAML.

Resultados

Após você enviar a solicitação de backup, a primeira operação de backup planejada será iniciada dentro da janela que é definida pela política do SLA. O horário de início do backup é registrado no status de backup.

O que Fazer Depois

Para visualizar informações sobre a solicitação de backup, emita o comando **kubectl describe** usando o nome da solicitação. Por exemplo, para visualizar informações sobre uma solicitação de backup que é denominada `backup-red-label` no espaço de nomes `baas`, emita o seguinte comando:

```
kubectl describe baasreq backup-red-label -n baas
```

Para obter instruções, consulte [“Visualizando o status de tarefas de backup e restauração”](#) na página 351.

Modificando parâmetros em um arquivo do YAML:

Depois que as tarefas de backup por rótulo planejadas tiverem sido iniciadas, é possível modificar o parâmetro SLA no arquivo YAML e aplicá-lo no mesmo rótulo, se necessário. Por exemplo:

- Para designar uma política de SLA diferente ao rótulo ou remover uma designação de SLA, edite os valores no campo **sla** no arquivo YAML. Em seguida, aplique o arquivo do YAML usando a interface da linha de comandos **kubectl**.

- Se você não quiser mais que as PVCs associadas a um rótulo participem de quaisquer tarefas de backup planejadas, remova as designações de política do SLA atualizando o campo **sla** no arquivo YAML. Para remover o rótulo de todos os SLAs, modifique o campo **sla** da seguinte forma:

```
sla: []
```

Em seguida, aplique o arquivo do YAML usando a interface da linha de comandos **kubectl**.

- Se você deseja modificar quaisquer outros parâmetros, deve-se criar uma nova solicitação e especificar um nome de solicitação diferente (*name_of_request*) no arquivo YAML.

Conceitos relacionados

[“Tipos de Backup e Restauração” na página 318](#)

O Suporte de Backup de Kubernetes fornece vários tipos de funções de backup e restauração. É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou a linha de comandos do Kubernetes para iniciar operações de backup e restauração.

[“Políticas de SLA” na página 319](#)

As políticas de acordo de nível de serviço (SLA) definem com que frequência as operações de backup de captura instantânea e backup de cópia são executadas e por quanto tempo são retidos. Também é possível configurar SLAs customizados que atendem aos seus requisitos operacionais.

[“Pedidos do Suporte de Backup de Kubernetes” na página 336](#)

Para proteger os dados do contêiner, é possível enviar solicitações do Suporte de Backup de Kubernetes usando a interface da linha de comandos do Kubernetes.

[“Resolução de Problemas do Suporte de Backup de Kubernetes” na página 534](#)

Para ajudar a solucionar problemas com Suporte de Backup de Kubernetes, é possível coletar arquivos de log de depuração e visualizar logs de rastreamento. Também é possível seguir procedimentos para diagnosticar problemas.

Fazendo backup de volumes persistentes por espaço de nomes usando a linha de comandos

É possível criar solicitações de backup para volumes persistentes especificando um espaço de nomes. Um cluster físico pode ser dividido em clusters virtuais que são chamados de espaços de nomes. Ao especificar um espaço de nomes em uma solicitação de backup, você pode fazer backup de todas as PVCs nesse espaço de nomes.

Antes de Iniciar

As solicitações de backup são direcionadas a solicitações de volume persistentes (PVCs) para os volumes que você deseja proteger. Antes de planejar uma tarefa de backup, tome as ações a seguir:

- Assegure-se de que a PVC exista dentro do espaço de nomes especificado.
- Assegure-se de que o PVC esteja formatado. Os PVCs devem ser formatados antes que possam ser submetidos a backup. Para que um PVC seja formatado corretamente, ele deve ser montado e gravado para. As operações de backup de volumes de bloco brutos não são suportadas.
- Determine qual política de SLA atribuir a PVCs. Para obter instruções sobre como visualizar as políticas de SLA disponíveis, consulte [“Políticas de SLA” na página 319](#).

Procedimento

1. Opcional: Exiba a lista de PVCs no espaço de nomes do qual você deseja fazer backup emitindo o seguinte comando:

```
kubectl get pvc -n namespace
```

2. Crie um arquivo YAML que defina a solicitação para a operação de backup por espaço de nomes. O arquivo do YAML deve conter as propriedades a seguir:

```
#-----  
# Filename: filename.yaml  
#-----
```

```

apiVersion: "baas.io/v1alpha1"
tipo: BaaSReq

metadados:
  name: name_of_request
  namespace: namespace
spec:
  requesttype: BackupNamespace
  sla: [sla_policy]
  volumesnapshotclass: snapshot_class_name

```

em que:

filename

Especifica o nome do arquivo de configuração do YAML. O tipo de arquivo é .yaml.

name_of_request

Especifica o nome da solicitação de backup por espaço de nomes. O nome deve ser exclusivo e não deve corresponder ao nome do PVC.

namespace

Especifica o espaço de nomes ao qual você deseja designar uma política de acordo de nível de serviço (SLA).

Depois de designar o SLA no nível do espaço de nomes, quaisquer novas PVCs criadas nesse espaço de nomes serão automaticamente designadas ao SLA.

[sla_policy]

Especifica a política de SLA que determina o planejamento para operações de backup. Você pode especificar mais de uma política de SLA usando uma lista separada por vírgula dentro dos colchetes.

Por exemplo, para designar a política *daily* para um PVC, especifique a instrução a seguir:

```
sla: [diário]
```

Para designar as políticas *every4hours*, *daily_midnight* e *weekly* para a PVC, especifique a instrução a seguir no arquivo YAML:

```
sla: [every4hours,daily_midnight,weekly]
```

Como alternativa, é possível usar o seguinte formato para especificar uma única política de SLA:

```
sla:
- daily
```

Ou use o formato a seguir para especificar várias políticas de SLA:

```
sla:
- every4hours
- daily_midnight
- weekly
```

Assegure-se de usar o caso correto ao especificar o nome da política de SLA. Os nomes da política fazem distinção entre maiúsculas e minúsculas em arquivos do YAML.

Para remover todas as designações de SLA de um espaço de nomes, exclua os nomes de políticas de SLA dentro dos suportes, conforme mostrado na seguinte instrução:

```
sla: []
```

snapshot_class_name

Especifica a classe de captura instantânea para o volume. Se você não especificar a classe de captura instantânea, a classe de captura instantânea padrão será usada se o contêiner sidecar *csi-snapshotter* na classe de captura instantânea padrão corresponder ao fornecedor do volume. Caso contrário, a solicitação de backup é inválida.

3. Envie a solicitação de backup emitindo o comando a seguir:


```
kubectl create -f filename.yaml
```

em que *filename* é o nome do arquivo de configuração do YAML.

Resultados

Após você enviar a solicitação de backup, a primeira operação de backup planejada será iniciada dentro da janela que é definida pela política do SLA. O horário de início do backup é registrado no status de backup.

O que Fazer Depois

Para visualizar informações sobre a solicitação de backup, emita o comando **kubectl describe** usando o nome da solicitação. Por exemplo, para visualizar informações sobre uma solicitação de backup denominada backup-namespace1 no espaço de nomes baas, emita o seguinte comando:

```
kubectl describe baasreq backup-namespace1 -n baas
```

Para obter instruções, consulte [“Visualizando o status de tarefas de backup e restauração” na página 351](#).

Modificando parâmetros em um arquivo do YAML:

Após as tarefas planejadas de backup por espaço de nomes serem iniciadas, é possível modificar o parâmetro SLA no arquivo YAML e aplicá-lo no mesmo espaço de nomes, se necessário. Por exemplo:

- Para designar uma política de SLA diferente para o espaço de nomes ou remover uma atribuição de SLA, edite os valores no campo **sla** no arquivo YAML. Em seguida, aplique o arquivo do YAML usando a interface da linha de comandos **kubectl**.
- Se você não quiser mais que as PVCs em um espaço de nomes participem de quaisquer tarefas de backup planejadas, remova as designações de política do SLA atualizando o campo **sla** no arquivo YAML. Para remover o espaço de nomes de todos os SLAs, modifique o campo **sla** da seguinte forma:

```
sla: []
```

Em seguida, aplique o arquivo do YAML usando a interface da linha de comandos **kubectl**.

- Se você deseja modificar qualquer outro parâmetro, deve-se criar uma nova solicitação e especificar um nome de solicitação diferente (*name_of_request*) no arquivo YAML.

Conceitos relacionados

[“Tipos de Backup e Restauração” na página 318](#)

O Suporte de Backup de Kubernetes fornece vários tipos de funções de backup e restauração. É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou a linha de comandos do Kubernetes para iniciar operações de backup e restauração.

[“Políticas de SLA” na página 319](#)

As políticas de acordo de nível de serviço (SLA) definem com que frequência as operações de backup de captura instantânea e backup de cópia são executadas e por quanto tempo são retidos. Também é possível configurar SLAs customizados que atendem aos seus requisitos operacionais.

[“Pedidos do Suporte de Backup de Kubernetes” na página 336](#)

Para proteger os dados do contêiner, é possível enviar solicitações do Suporte de Backup de Kubernetes usando a interface da linha de comandos do Kubernetes.

[“Resolução de Problemas do Suporte de Backup de Kubernetes” na página 534](#)

Para ajudar a solucionar problemas com Suporte de Backup de Kubernetes, é possível coletar arquivos de log de depuração e visualizar logs de rastreamento. Também é possível seguir procedimentos para diagnosticar problemas.

Restaurando dados do contêiner usando a linha de comandos

Você pode usar a interface da linha de comandos do Kubernetes para restaurar um volume persistente a partir de um backup de captura instantânea ou um backup de cópias. Uma operação de restauração de captura instantânea geralmente é mais rápida do que uma operação de restauração de cópia.

Antes de Iniciar

Revise as seguintes restrições:

- Para qualquer tipo de operação de restauração, não é possível restaurar um volume para um espaço de nomes ou cluster diferente.
- É possível restaurar um backup de captura instantânea ou de cópia apenas para um novo volume persistente. A solicitação de volume persistente (PVC) para o novo volume é criada automaticamente quando você restaura o backup de captura instantânea ou cópia.
- Para assegurar que uma solicitação de restauração funcione corretamente, não exclua manualmente quaisquer capturas instantâneas de volumes que sejam protegidas por Suporte de Backup de Kubernetes.

Sobre Esta Tarefa

Dependendo do objetivo do ponto de recuperação e do objetivo do tempo de recuperação, é possível executar uma operação de restauração rápida ou restauração de cópia:

- Para restaurar um volume no menor tempo possível, execute uma operação de restauração rápida para restaurar uma captura instantânea. Se outra operação estiver em andamento no mesmo volume, a operação de restauração rápida poderá demorar mais para ser concluída.
- Para restaurar um volume em um momento especificado no servidor vSnap do IBM Spectrum Protect Plus, execute uma operação de restauração de cópia.

Procedimento

1. Para visualizar os pontos de restauração que estão disponíveis para uma PVC, consulte todos os backups para a PVC executando o seguinte comando:

```
kubect1 describe BaaSReq pvc_name -n namespace
```

Os pontos de restauração são identificados pelo registro de data e hora do backup de captura instantânea ou cópia.

2. Na saída de status que é exibida, identifique o registro de data e hora do backup de captura instantânea ou cópia de cópia que deseja restaurar. Os registros de data e hora são mostrados na seção Status da saída antes do tipo de backup.

Por exemplo, a saída a seguir mostra os registros de data e hora para diferentes tipos de backups:

```
Status:
Timestamp: 2019-05-30 13:27:21
Type:      FAST
Timestamp: 2019-05-30 13:32:21
Type:      COPY
```

em que:

FAST

Denota o tipo de backup para uma captura instantânea que é feita durante uma operação de backup de captura instantânea.

COPY

Denota o tipo de backup para um backup de cópia que é armazenado em um servidor vSnap do IBM Spectrum Protect Plus.

3. Para especificar a solicitação de restauração, crie um arquivo YAML com as propriedades a seguir. Insira o registro de data e hora para a captura instantânea de origem no parâmetro **restorepoint**.

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: name_of_restore_request  
  namespace: namespace  
spec:  
  requesttype: restore  
  pvcname: pvc_name  
  targetvolume: target_volume_for_restore  
  storageclass: storage_class_of_target_volume  
  restorepoint: timestamp_of_backup  
  restoretype: fast | copy
```

em que:

filename

Especifica o nome do arquivo de configuração do YAML.

name_of_restore_request

Especifica o nome da solicitação para a tarefa de restauração. O nome deve ser exclusivo e não deve corresponder ao nome da PVC.

Uma nova solicitação de restauração deve ser criada para cada restauração subsequente da mesma PVC. Em outras palavras, para restaurar uma PVC novamente, crie uma nova solicitação e especifique um nome de solicitação diferente (*name_of_request*) no arquivo YAML.

namespace

Especifica o espaço de nomes para a solicitação.

pvc_name

Especifica o nome da PVC que você deseja restaurar.

target_volume_for_restore

Especifica o nome da PVC para a qual deseja restaurar o volume.

Para restaurações rápidas ou restaurações de cópia, o volume é sempre restaurado para uma nova PVC. Nesse caso, forneça o nome da nova PVC.

storage_class_of_target_volume

Especifica a classe de armazenamento que é definida para o volume de destino.

Para operações de restauração rápida, a classe de armazenamento é ignorada. A classe de armazenamento da PVC original é usada.

Para operações de restauração de cópia, é possível especificar uma classe de armazenamento que é a mesma que a PVC original ou especificar uma classe de armazenamento diferente. Se você não especificar a classe de armazenamento, a classe de armazenamento da PVC original será usada.

Se você especificar uma classe de armazenamento, mas não especificar o tipo de restauração com o parâmetro **restoretype**, ocorrerá uma operação de restauração de cópia.

timestamp_of_backup

Especifica o registro de data e hora do backup de cópia ou de captura instantânea de origem do qual você deseja restaurar. O registro de data e hora está no formato Hora Universal Coordenada (UTC).

Se você não especificar um registro de data e hora, o backup de captura instantânea ou de cópia mais recente será restaurado.

restoretype: fast | copy

Especifica o tipo de operação de restauração a ser utilizado.

rápido

Restaura um volume a partir de um backup de captura instantânea.

cópia

Restaura um volume a partir de um backup de cópias.

Esse parâmetro é opcional. Se você não especificar um tipo de restauração, o tipo de restauração será determinado automaticamente. Se existir uma captura instantânea no registro de data e hora especificado, uma restauração rápida será executada para restaurar a captura instantânea. Se apenas um backup de cópia estiver disponível no momento especificado, uma restauração de cópia será executada para restaurar o backup de cópia.

4. Inicie a solicitação de restauração emitindo o comando a seguir:

```
kubect1 create -f filename.yaml
```

em que *filename* é o nome do arquivo de configuração do YAML.

O que Fazer Depois

Se você restaurou dados para um novo volume persistente, reconfigure o contêiner do aplicativo para montar o novo volume após o backup de captura instantânea ou de cópia ser restaurado.

Para gerenciar de forma mais eficiente suas solicitações do Suporte de Backup de Kubernetes, exclua as solicitações concluídas emitindo o seguinte comando:

```
kubect1 delete baasreq name_of_restore_request -n namespace
```

Ao excluir solicitações concluídas, você ganha os seguintes benefícios:

- O tamanho do banco de dados etcd é reduzido e você pode reutilizar o nome de uma solicitação para outra operação.
- O processo de resolução de problemas é simplificado.
- O rastreamento de solicitações de backup e restauração é simplificado. A qualquer momento, é possível obter uma lista precisa de solicitações que estão em execução em seu cluster quando você emitir o seguinte comando:

```
kubect1 get baasreq -n namespace
```

Conceitos relacionados

[“Tipos de Backup e Restauração” na página 318](#)

O Suporte de Backup de Kubernetes fornece vários tipos de funções de backup e restauração. É possível usar a interface com o usuário do IBM Spectrum Protect Plus ou a linha de comandos do Kubernetes para iniciar operações de backup e restauração.

[“Pedidos do Suporte de Backup de Kubernetes” na página 336](#)

Para proteger os dados do contêiner, é possível enviar solicitações do Suporte de Backup de Kubernetes usando a interface da linha de comandos do Kubernetes.

[“Resolução de Problemas do Suporte de Backup de Kubernetes” na página 534](#)

Para ajudar a solucionar problemas com Suporte de Backup de Kubernetes, é possível coletar arquivos de log de depuração e visualizar logs de rastreo. Também é possível seguir procedimentos para diagnosticar problemas.

Tarefas relacionadas

[“Visualizando o status de tarefas de backup e restauração” na página 351](#)

Depois de enviar uma solicitação de backup ou restauração, é possível usar os comandos **kubect1 get** e **kubect1 describe** para mostrar informações sobre o sua solicitação.

Gerenciando tarefas de backup e restauração de contêiner

É possível consultar informações sobre tarefas de backup e restauração e excluir backups de captura instantânea e de cópia que não são mais necessários.

Visualizando o status de tarefas de backup e restauração

Depois de enviar uma solicitação de backup ou restauração, é possível usar os comandos **kubect1 get** e **kubect1 describe** para mostrar informações sobre o sua solicitação.

Procedimento

1. Para mostrar uma listagem de todas as solicitações do Suporte de Backup de Kubernetes em um espaço de nomes, emita o comando **kubect1 get** da seguinte forma:

```
kubect1 get baasreq -n namespace
```

Por exemplo, para mostrar todas as solicitações no espaço de nomes `production-01`, emita o comando a seguir:

```
kubect1 get baasreq -n production-01
```

A saída é semelhante ao seguinte exemplo:

NAME	AGE
vol08-adhoc	17d
inv-adhoc2	17d
db-vol08	18d
db-vol09	17d

Os nomes da solicitação estão listados na coluna `NOME` da saída.

2. Usando os resultados da Etapa “1” na página 351, emita o comando **kubect1 describe** para mostrar o status de uma tarefa. Por exemplo:

- Para mostrar a lista de todos os backups para qualquer solicitação, incluindo backups de solicitações de backup planejado e on demand, especifique o nome da solicitação e o espaço de nomes no comando a seguir:

```
kubect1 describe baasreq request_name -n namespace
```

em que *request_name* é o nome da solicitação. Para backups on demand, use o nome da PVC como o nome da solicitação.

Por exemplo, para mostrar todos os backups para PVC `db-vol08` no espaço de nomes `production-01`, emita o seguinte comando:

```
kubect1 describe baasreq db-vol08 -n production-01
```

A saída é semelhante ao seguinte exemplo:

```
kubectl describe baasreq db-vol08 -n production-01
Name:          db-vol08
Namespace:     production-01
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  Ready
Kind:          BaaSReq
Metadata:
  Creation Timestamp:  2020-05-20T20:28:33Z
  Generation:         9
  Resource Version:    2955966
  Self Link:           /apis/baas.io/v1alpha1/namespaces/production-01/baasreqs/db-vol08
  UID:                0e8d4412-522f-44b3-932c-1e6239f7bf8e
Spec:
  Inprogress:  None
  Instanceid:  e05c400868ab9151e3c792d28edfbb18
  Origreqtype: backup
  Requesttype: backup
  Size:        1073741824
  Sla:
    joanne-copy2
  Spppvname:      cluster01:production-01:db-vol08
  Volumesnapshotclass:  cirrus-csi-rbdplugin-snapclass
Status:
  Snapshotname:  spp-1005-2161-172342eb32d
  Timestamp:     2020-05-20 22:24:25
  Type:          FAST
  Snapshotname:  2000.snapshot.824
  Timestamp:     2020-05-20 21:13:27
  Type:          COPY
  Snapshotname:  spp-1005-2161-17233c4e7a0
  Timestamp:     2020-05-20 20:28:14
  Type:          FAST
```

- Para mostrar informações sobre uma tarefa de restauração, emita o comando a seguir:

```
kubectl describe baasreq request_name -n namespace
```

em que *request_name* é o nome da solicitação da tarefa de restauração e *namespace* é o espaço de nomes da PVC que foi restaurada.

Resultados

Na saída de comando, o campo **Backupstatus** mostra o status de uma tarefa de backup. Para tarefas de restauração, o campo **Restorestatus** mostra o status da tarefa de restauração. Para obter mais informações, consulte [“Status das tarefas de backup e restauração” na página 352](#).

O campo **instanceid** contém uma sequência gerada aleatoriamente que identifica com exclusividade um volume em IBM Spectrum Protect Plus.

O campo **Spppvname** mostra o nome da PVC que é relatado na janela IBM Spectrum Protect Plus **Tarefas e Operações**. O formato *namespace:pvc_name* é usado para identificar a PVC. Os valores para os campos **instanceid** e **Spppvname** identificam com exclusividade um backup em IBM Spectrum Protect Plus.

Em solicitações de backup, a seção **Status** mostra a lista de backups que foram concluídos. Para cada backup, o registro de data e hora do backup é listado, seguido pelo tipo de backup que foi executado. Os tipos de backups são definidos da seguinte forma:

FAST

Denota o tipo de backup para uma captura instantânea que é feita durante uma operação de backup de captura instantânea.

COPY

Denota o tipo de backup para um backup de cópia que é armazenado em um servidor vSnap do IBM Spectrum Protect Plus.

Status das tarefas de backup e restauração

Ao usar o comando **kubectl describe** para mostrar informações sobre tarefas de backup e restauração, o status das tarefas de backup e restauração é exibido na saída de comando.

Para exibir o status de uma solicitação do Suporte de Backup de Kubernetes específica, insira o comando a seguir:

```
kubectrl describe baasreq request_name -n namespace
```

em que *request_name* é o nome da solicitação e *namespace* é o espaço de nomes no qual o volume persistente existe. Para obter mais informações, consulte [“Visualizando o status de tarefas de backup e restauração” na página 351](#).

Status de backup relatado

O status de uma tarefa de backup é mostrado no campo Backupstatus na saída de comando. A tabela a seguir mostra os possíveis status de uma solicitação de backup:

Tabela 60. Status das tarefas de backup	
Status de Backup	Descrição
Nenhuma	Nenhuma tarefa de backup foi iniciada para este planejamento.
Solicitado	Uma tarefa de backup foi iniciada para este planejamento.
Ready	Pelo menos uma tarefa de backup foi concluída para este planejamento.
Destruído	Todos os backups de captura instantânea e cópia de uma solicitação de volume persistente foram excluídos.
Inválida	Ocorreu um problema com a solicitação. Uma explicação possível está listada no campo Errmsg .

Status de restauração relatado

O status de uma tarefa de restauração é mostrado no campo Restorestatus na saída de comando. A tabela a seguir mostra os possíveis status de uma tarefa de restauração:

Tabela 61. Status de tarefas de restauração	
Restaurar status	Descrição
Nenhuma	Nenhuma tarefa de restauração foi solicitada.
Solicitado	É solicitada uma tarefa de restauração de backup de cópia ou captura instantânea.
Restaurada	Uma captura instantânea ou um backup de cópia foi restaurado com sucesso.
Inválida	Ocorreu um problema com a solicitação. Uma explicação possível está listada no campo Errmsg .

Excluindo backups de contêiner

Você pode marcar para exclusão os backups de cópia e captura instantânea de uma solicitação de volume persistente (PVC) enviando uma solicitação **destroy**.

Antes de Iniciar

Antes de enviar uma solicitação **destroy** para excluir backups de contêiner, considere as seguintes consequências:

- Todas as capturas instantâneas de PVC são excluídas quando suas datas de expiração são atingidas, conforme definido pela política de acordo de nível de serviço (SLA) para a PVC.
- Os backups de captura instantânea e de cópia no servidor vSnap do IBM Spectrum Protect Plus serão marcados para exclusão. A exclusão é gerenciada pelo IBM Spectrum Protect Plus.
- A solicitação de backup original não será excluída pela solicitação **destroy**. Você deve executar o comando **kubectl delete** para excluí-lo.
- A solicitação **destroy** não é suportada para backups on demand. Use o comando **kubectl delete** para excluir uma solicitação de backup on demand. Uma captura instantânea on demand é excluída quando a captura instantânea expira ou quando o backup planejado é destruído.

Procedimento

1. Crie um arquivo YAML para a solicitação **destroy** que contém as propriedades a seguir:

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
tipo: BaaSReq

metadados:
  nome: request_name
  namespace: namespace
spec:
  requesttype: Destroy
```

em que:

filename

O nome do arquivo de configuração YAML.

request_name

O nome da solicitação, que deve corresponder ao nome da PVC que foi submetida a backup. Por exemplo, se você deseja excluir todos backups de captura instantânea e de cópia para a PVC denominada db-vol01, o nome da solicitação também deve ser db-vol01.

namespace

O espaço de nomes no qual o PVC existe.

2. Envie a solicitação **destroy**, inserindo o comando a seguir na linha de comandos:

```
kubectl apply -f filename.yaml
```

em que *filename* é o nome do arquivo de configuração do YAML.

3. Para verificar se os backups de captura instantânea e de cópia para uma PVC são excluídas, emita o seguinte comando:

```
kubectl describe baasreq request_name -n namespace | grep Backupstatus
```

em que *request_name* é o nome do PVC que foi submetido a backup.

Na saída de comando, o status a seguir mostra que os backups foram excluídos:

```
Backupstatus: Destroyed
```

O que Fazer Depois

Como uma melhor prática, exclua a solicitação concluída emitindo o comando a seguir:

```
kubectl delete baasreq request_name -n namespace
```

em que *request_name* é o nome do PVC que foi submetido a backup.

Ao excluir solicitações concluídas, você ganha os seguintes benefícios:

- O tamanho do banco de dados etcd é reduzido e você pode reutilizar o nome de uma solicitação para outra operação.
- O processo de resolução de problemas é simplificado.
- O rastreamento de solicitações de backup e restauração é simplificado. A qualquer momento, é possível obter uma lista precisa de solicitações que estão em execução em seu cluster quando você emitir o seguinte comando:

```
kubect1 get baasreq -n namespace
```

Se você excluir a solicitação de backup sem primeiro destruir o backup, a solicitação de backup continuará a ser executada e os backups serão feitos de acordo com a política de SLA especificada até que o Suporte de Backup de Kubernetes seja reiniciado.

Informações relacionadas

[“Tipos de solicitações no Suporte de Backup de Kubernetes” na página 336](#)

Capítulo 13. Proteger dados em sistemas em nuvem

Os sistemas em nuvem, como o Microsoft Office 365, podem ser registrados com IBM Spectrum Protect Plus para que você possa começar a proteger seus dados. Registre o Office 365 com IBM Spectrum Protect Plus para que você possa configurar tarefas de backup ou políticas regulares de acordo de nível de serviço (SLA) regulares.

Se optar por proteger o Microsoft Office 365 com IBM Spectrum Protect Plus, você precisa comprar IBM Spectrum Protect Plus para Microsoft Office 365 Entity ID Monthly License, Número da Peça D25ZELL. Para obter mais informações sobre essa titularidade, consulte a carta de anúncio do [IBM Spectrum Protect Plus V10.1.5](#).

Microsoft Office 365

Para proteger o e-mail, os calendários, os contatos e os dados do Microsoft Office 365 em um armazenamento em nuvem OneDrive, primeiro deve-se registrar o aplicativo Office 365 com o Azure Active Directory. Em seguida, implemente o servidor de aplicativos e registre-o com IBM Spectrum Protect Plus. Depois disso, deve-se incluir os locatários do Office 365 e definir uma política de acordo de nível de serviço (SLA) para criar tarefas de backup.

É possível usar o IBM Spectrum Protect Plus para registrar e testar dados do Office 365 em um ambiente não produtivo. Se você optar por proteger o Microsoft Office 365 em um ambiente produtivo com o IBM Spectrum Protect Plus, será necessário adquirir a Licença Mensal do IBM Spectrum Protect Plus for Microsoft Office 365 Entity ID, Número de Peça D25ZELL. Para obter mais informações sobre essa titularidade, consulte a carta de anúncio do [IBM Spectrum Protect Plus V10.1.5](#). Observe que este é um link externo.

Registrando com o Azure Active Directory

Para proteger um aplicativo Office 365, deve-se registrar o aplicativo com o Azure Active Directory e conceder permissões apropriadas. Quando você registrar um novo aplicativo com o Azure Active Directory, as credenciais do aplicativo como ID do aplicativo e o segredo do aplicativo serão disponibilizadas no portal do Azure Active Directory.

Antes de Iniciar

Execute as seguintes ações:

- Assegure-se de que você tenha uma assinatura ativa do Office 365.
- Assegure-se de que você tenha um ID do usuário administrativo e uma senha do Office 365.

Procedimento

1. Acesse a página de boas-vindas do Office 365 e conecte-se à sua conta da Microsoft usando o ID do usuário administrativo e a senha do Office 365.
2. Para abrir o centro administrativo do Azure Active Directory, na área de janela esquerda, clique nas reticências para expandir o menu **Mostrar Todos** e, em seguida, clique em **Centros de Administração > Azure Active Directory**.
3. Para abrir o seu painel de locatários, na área de janela esquerda do centro administrativo do Azure Active Directory, clique em **Azure Active Directory**.
4. No menu do painel do locatário, clique em **Registros de Aplicativo** e, em seguida, clique em **Novo Registro**.
5. Para especificar um nome para o usuário para o aplicativo Office 365, na página "Registrar um Aplicativo", digite um nome no campo **Nome**.
6. Use as opções padrão para os campos restantes e clique em **Registrar**. O registro do aplicativo é configurado com o nome para o usuário que você inseriu.

7. Para obter a sequência de ID de aplicativo (cliente) e ID de diretório (locatário), clique em **Azure Active Directory > - Registros de Aplicativo > Nome do Aplicativo**. Em seguida, copie a sequência de ID de aplicativo e ID de diretório. Essas sequências serão necessárias posteriormente quando você registrar o aplicativo Office 365 com o IBM Spectrum Protect Plus.
8. Para criar um segredo de cliente para esse ID de aplicativo, clique em **Certificados e Segredos > Novo Segredo do Cliente**.
9. Na área de janela "Incluir um Segredo de Cliente", insira qualquer nome de usuário no campo **Descrição** e clique em **Incluir**. Um segredo de cliente é gerado e o valor é então exibido na área de janela Segredos do Cliente.
10. Copie o segredo do cliente para a área de transferência usando o recurso de cópia ao lado do campo **Valor Secreto do Cliente**. Essa sequência de caracteres também é usada para registro com o IBM Spectrum Protect Plus.
11. Para incluir permissões para esse ID de aplicativo, clique em **Permissões de API > Incluir Permissões**.
12. Especifique permissões para cada API na tabela a seguir, tomando as seguintes ações. Selecione o nome da API, por exemplo, Azure Active Directory Graph.
 - a) Para o nome da permissão User.Read.All, selecione o tipo **Permissões Delegadas**.
 - b) Para obter as permissões restantes, selecione o tipo **Permissões de Aplicativo** para cada nome de permissão para a API na tabela.

API	Nome da permissão
Gráfico do Active Directory do Azure	User.Read.All
Gráfico do Active Directory do Azure	Directory.Read.All
Troca	full_access_as_app
Microsoft Graph	Calendars.ReadWrite
Microsoft Graph	Contacts.ReadWrite
Microsoft Graph	Files.ReadWrite.All
Microsoft Graph	Mail.ReadWrite
Microsoft Graph	Sites.Read.All
Microsoft Graph	User.Read
Microsoft Graph	User.Read.all

13. Para salvar as permissões selecionadas, clique em **Dar Consentimento Admin para <your organization name>**.

O que Fazer Depois

Siga as instruções em [“Registrando o locatário do Office 365 com IBM Spectrum Protect Plus”](#) na página 358.

Registrando o locatário do Office 365 com IBM Spectrum Protect Plus

Para assegurar que o agente IBM Spectrum Protect Plus possa se conectar ao locatário do Office 365, você deve registrar as credenciais do locatário do Office 365 e o servidor host proxy com IBM Spectrum Protect Plus. Esse procedimento é necessário para assegurar que os dados do Office 365 possam ser submetidos a backup para IBM Spectrum Protect Plus.

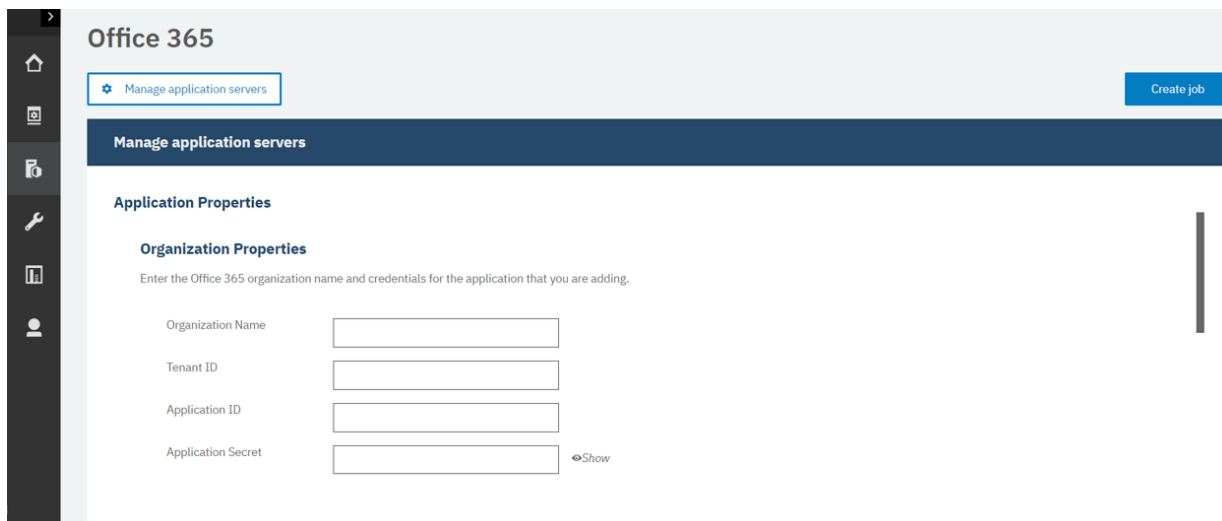
Antes de Iniciar

Assegure-se de que você tenha um sistema Linux que possa agir como a máquina de proxy de nuvem. O IBM Spectrum Protect Plus implementa o agente de backup nesta máquina. Para obter mais informações sobre os requisitos, consulte [Requisitos do Office 365](#). Assegure-se de que o aplicativo Office 365 esteja

registrado com o Azure Active Directory. Para obter instruções, consulte [“Registrando com o Azure Active Directory”](#) na página 357.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Gerenciamento de Nuvem > Office 365**.



2. Na página do Office 365, clique em **Gerenciar Servidores de Aplicativos** e, em seguida, clique em **Incluir Servidor de Aplicativos**.
3. Na página Propriedades da Organização, preencha os campos a seguir:
 - a. No campo **Nome da Organização**, digite o nome da organização que você configurou no centro administrativo do Azure Active Directory.

Nota: Esse é o nome da Organização/Locatário, como *tenantname.onmicrosoft.com*, e não é visualizável quando você está registrando o aplicativo Azure.
 - b. No campo **ID do Locatário**, insira a sequência do campo **ID do Diretório (Locatário)** no registro do aplicativo Azure Active Directory.
 - c. No campo **ID do Aplicativo**, insira a sequência do campo **ID do Aplicativo (Cliente)** no registro do aplicativo Azure Active Directory.
 - d. No campo **Segredo do Aplicativo**, insira a sequência de senha que foi gerada durante o registro do aplicativo Azure Active Directory.
4. Na página Propriedades do Proxy, preencha os campos a seguir:
 - a. No campo **Endereço de Host**, insira o nome do host ou IP do servidor Linux que está sendo usado como o host do proxy.
 - b. Para autenticação do servidor host, selecione uma das opções a seguir:
 - **Usuário:** selecione um usuário existente ou digite um ID do usuário e a senha associada.
 - **Chave SSH:** selecione uma chave de Shell Seguro (SSH) da lista suspensa.
5. Clique em **Save**.

Resultados

Quando um host do proxy é registrado no IBM Spectrum Protect Plus, um inventário é executado automaticamente na organização do Office 365, que retorna os usuários do Office 365 nesse recurso.

Logs de processo detalhados

O log de processo detalhado é um arquivo de log de processo do Microsoft O365 adicional que ajuda quando você está solucionando problemas. Esse log é coletado para rastrear todos os processos de backup e restauração para ajudar a resolução de problemas e para o rastreamento.

Um log de processo detalhado rastreia os processos para cada item do Office 365 protegido. Ao fazer o download do arquivo .zip do log da tarefa, é possível visualizar o arquivo de log do processo detalhado juntamente com arquivos de diagnóstico padrão.

Nota: Para localizar o log, faça o download do arquivo `joblog.zip`. Quando você descompactar os arquivos `diag.tar.gz`, localize o arquivo `Audit.log`. Esse é o arquivo com as informações de processamento do O365.

Conteúdo do log de processo detalhado e exemplo

Um arquivo de log de processo detalhado inclui as informações a seguir:

- Data e hora da operação.
- Tipo de operação.
- Conta que está associada à operação.
- Indicação que diz se o evento se relaciona ao OneDrive, a uma mensagem, a um evento ou a um contato.
- Mensagens informativas:
 - Para OneDrive, o caminho e o nome de arquivo do objeto processado são listados. Se a operação for uma operação de restauração redirecionada, isso é indicado.
 - Para as mensagens, é listada a data e a hora da mensagem. Se a operação for uma operação de restauração redirecionada, quaisquer mensagens associadas serão listadas.
 - Para eventos, o assunto do evento é listado.
 - Para contatos, o nome do contato é listado.

Exemplo de log de processo detalhado

As informações no log de processo detalhado são fornecidas no formato a seguir:

```
[date time] [operation] [account] [relation] [message1] optional: [message2]
```

Por exemplo,

```
2020-02-13 19:15:27.805 Backup Completed username@example.com OneDrive
"my_new_document.pdf"
2020-02-13 19:13:46.754 Backup Completed username@example.com Message "1/20/2020 10:52:01
PM +01:00" "Welcome!"
2020-02-13 19:16:14.196 Backup Completed username@example.com Contact "John Smith"
2020-02-13 19:14:48.847 Backup Completed username@example.com Event "Monday meeting"
2020-02-13 19:18:22.544 Backup Failed username@example.com OneDrive "my_folder
\inventory.pdf"
2020-02-13 19:15:27.805 Restore Completed username@example.com OneDrive
"my_new_document.pdf" "my_new_document_2020-02-11_19_15.pdf"
2020-02-13 19:22:28.238 Backup Failed username@example.com OneDrive "my_folder\inv
\inventory.pdf"
```

Fazendo backup de dados do Office 365

Após a organização do seu Office 365 ser registrada com IBM Spectrum Protect Plus, é possível aplicar uma política de acordo de nível de serviço (SLA) para começar a proteger os dados do Office 365.

Procedimento

1. Na área de janela de navegação do IBM Spectrum Protect Plus, expanda **Gerenciar Proteção > Gerenciamento de Nuvem > Office 365**.

2. Marque a caixa de seleção para a organização.
3. Clique em **Selecionar uma política de SLA** e escolha uma política de SLA.
Para obter informações adicionais sobre políticas de SLA, consulte [“Criar políticas de backup”](#) na página 163.
4. Salve sua opção. Para definir um novo SLA ou para editar uma política existente com períodos de retenção customizados ou taxas de frequência de backup, clique em **Gerenciar Proteção > Visão Geral de Política**. Na área de janela "Políticas de SLA", clique em **Incluir Política de SLA** e defina as preferências de política.

Nota: Algumas opções no campo **Opções de Política** na seção **Status da Política de SLA** diferem em disponibilidade com base no tipo de backup.
5. Para executar a política fora da tarefa planejada, execute as seguintes ações.
 - a. Para fazer backup de todos os dados da organização, marque a caixa de seleção para a organização.
 - b. Para fazer backup de dados de uma conta, clique em Organização e marque a caixa de seleção para o nome do usuário que está associado à conta.
 - c. Para fazer backup de e-mail, calendários, contatos ou dados do OneDrive para uma conta, clique em Organização e, em seguida, clique no nome do usuário e marque a caixa de seleção para o e-mail, calendário, contatos ou OneDrive para fazer backup.
6. Clique em **Executar**. O status muda para **Em Execução** para o seu SLA escolhido e você pode acompanhar o progresso da tarefa no log.

Backup incremental contínuo para o Office 365

O IBM Spectrum Protect Plus fornece uma estratégia de backup chamada *incremental contínua*. Em vez de planejar tarefas de backup completo periódicas, essa 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 objetos que são novos ou que foram alterados 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 faz backup de todos os dados das contas selecionadas do Office 365.
2. Todas as tarefas de backup subsequentes fazem backup apenas de dados novos ou alterados das contas selecionadas.

Restaurando dados do Office 365

É possível restaurar dados do Office 365 de cópias de backup em servidores vSnap ou armazenamento remoto. Quando você estiver pronto para restaurar uma caixa de correio para o Office 365, é possível concluir a tarefa no IBM Spectrum Protect Plus.

Antes de Iniciar

Pelo menos uma tarefa de backup do Office 365 deve ter sido executada com sucesso. Para obter instruções sobre como configurar uma tarefa de backup, consulte [“Fazendo backup de dados do Office 365”](#) na página 360.



Sobre Esta Tarefa

Os seguintes modos de restauração são suportados:

- Restaurar dados para a conta original
- Restaurar dados para outra conta

- Restaurar dados para um caminho especificado

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Gerenciamento de Nuvem > Office 365**.
2. Clique em **Criar tarefa**.
3. Selecione **Restaurar**.
4. Na área de janela **Selecionar Origem**, conclua as etapas a seguir:
 - a) Clique em uma origem na lista para exibir os dados que podem ser restaurados para a organização selecionada. Também é possível usar a função de procura para procurar dados disponíveis e alternar os dados exibidos usando o filtro **Visualizar**.
 - b) Para selecionar dados para restaurar, clique no ícone Incluir na lista de restauração  ao lado dos dados. Você pode selecionar mais de um item da lista. Os itens selecionados são incluídos na lista de restauração. Para remover um item da lista de origem, clique no ícone Remover da lista de restauração  ao lado dos dados.
 - c) Clique em **Avançar** para continuar.
5. Na página "Captura instantânea de origem", selecione o tipo de restauração e o horário em que os dados a serem restaurados foram submetidos a backup. Em seguida, clique em **Avançar** para continuar.
6. Na página "Selecionar destino", preencha os campos a seguir e clique em **Avançar** para continuar.

Opção	Descrição
Selecione um destino	Selecione o local para o qual os dados devem ser restaurados: Restaurar para a conta original Restaura dados para a conta original do Office 365 Restaurar para outra conta Restaura dados para outra conta do Office 365
Restaurar caminho	Restaura dados para o caminho do diretório selecionado na conta do Office 365
7. Na página **Opções de Tarefa**, se quiser executar operações de restauração em fluxos paralelos, especifique um valor no campo **Máximo de Fluxos Paralelos**. Em seguida, clique em **Avançar** para continuar.
8. Na página Revisão, revise as configurações da tarefa de restauração.
9. Para iniciar a tarefa de restauração, clique em **Enviar**.

Resultados

Alguns momentos depois de clicar em **Enviar**, a tarefa de restauração on demand é incluída na guia Tarefas em Execução na página Tarefas e Operações. É possível clicar no registro da tarefa para exibir os detalhes da operação. Também é possível fazer download do arquivo de log compactado clicando em **Download.zip**.

O nome da conta para os dados restaurados pode ser encontrado no arquivo de log para a operação de restauração. Para localizar os logs para uma operação de restauração, na área de janela de navegação, clique em **Tarefas e Operações** e, em seguida, clique na guia **Tarefas em Execução**.

Capítulo 14. Protegendo bancos de dados

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.

Restrição: O IBM Spectrum Protect Plus pode criar pastas nos servidores de aplicativos quando os aplicativos forem registrados com IBM Spectrum Protect Plus. As pastas criadas por IBM Spectrum Protect Plus devem permanecer para que o produto funcione corretamente. No entanto, se você tiver que remover uma pasta que foi criada por IBM Spectrum Protect Plus, cancele o registro do aplicativo e o IBM Spectrum Protect Plus irá limpar as pastas associadas ao registro.

Não designe mais de um aplicativo por máquina como um servidor de aplicativos para um grupo de recursos. Por exemplo, se o Microsoft SQL Server e o Microsoft Exchange Server ocupam a mesma máquina e ambos são registrados com IBM Spectrum Protect Plus, apenas um dos aplicativos pode ser incluído como um servidor de aplicativos para um determinado grupo de recursos.

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 60.

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 367.

O endereço IP deve ser alcançável a partir do servidor IBM Spectrum Protect Plus e do servidor vSnap. Ambos devem ter um serviço Windows Remote Management atendendo na porta 5985.

O nome completo do domínio deve ser resolvível e roteável a partir do servidor de dispositivo IBM Spectrum Protect Plus e do servidor vSnap.

Pré-requisitos para o Db2

Todos os pré-requisitos para o Servidor de aplicativos IBM Spectrum Protect Plus Db2 devem ser atendidos antes de você começar a proteger recursos do Db2 com o IBM Spectrum Protect Plus.

Os requisitos para o Servidor de aplicativos IBM Spectrum Protect Plus 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.
- 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 arquivos maiores 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 366.
- Em um ambiente Linux, assegure-se de que o pacote do utilitário Linux, **util-linux-ng**, ou o pacote **util-linux** seja atual.
- 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.

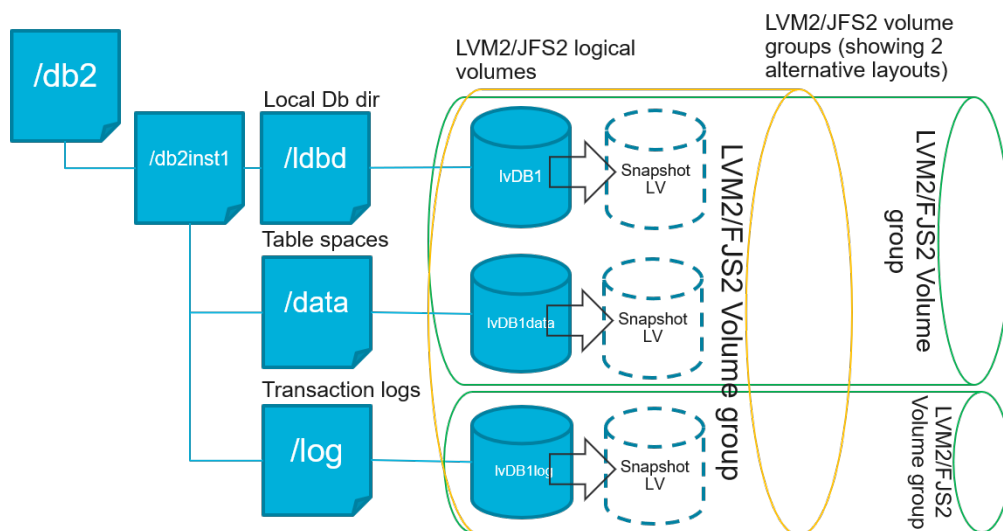


Figura 35. Exemplos de Layout de Volume Lógico

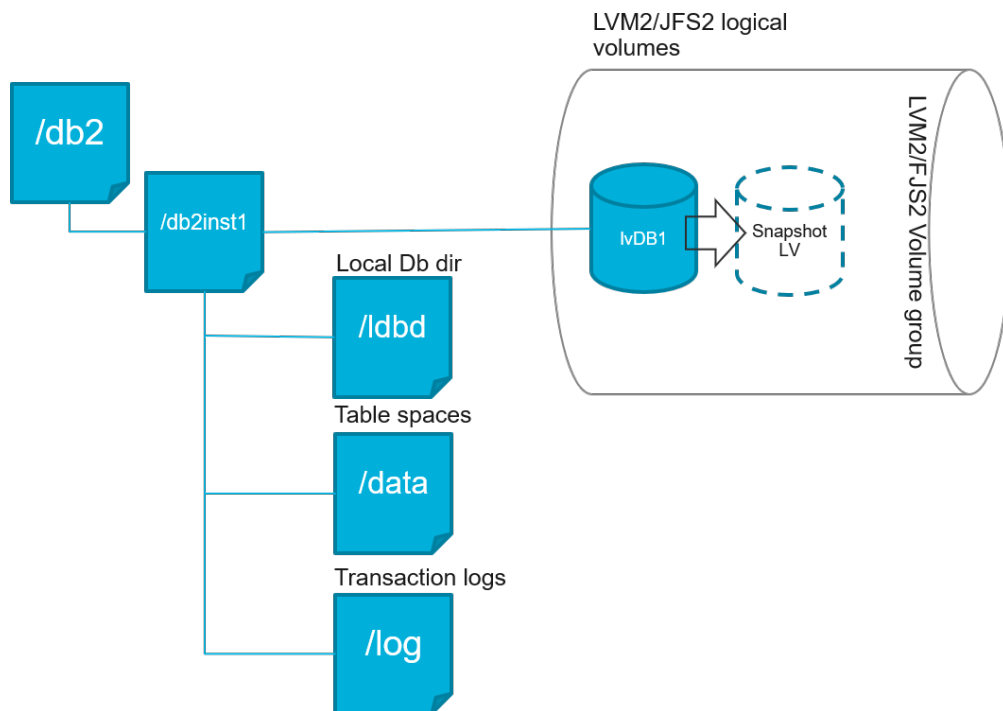


Figura 36. Exemplo de Layout de Volume Lógico Único

- 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 37. 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 38. 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. 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**.

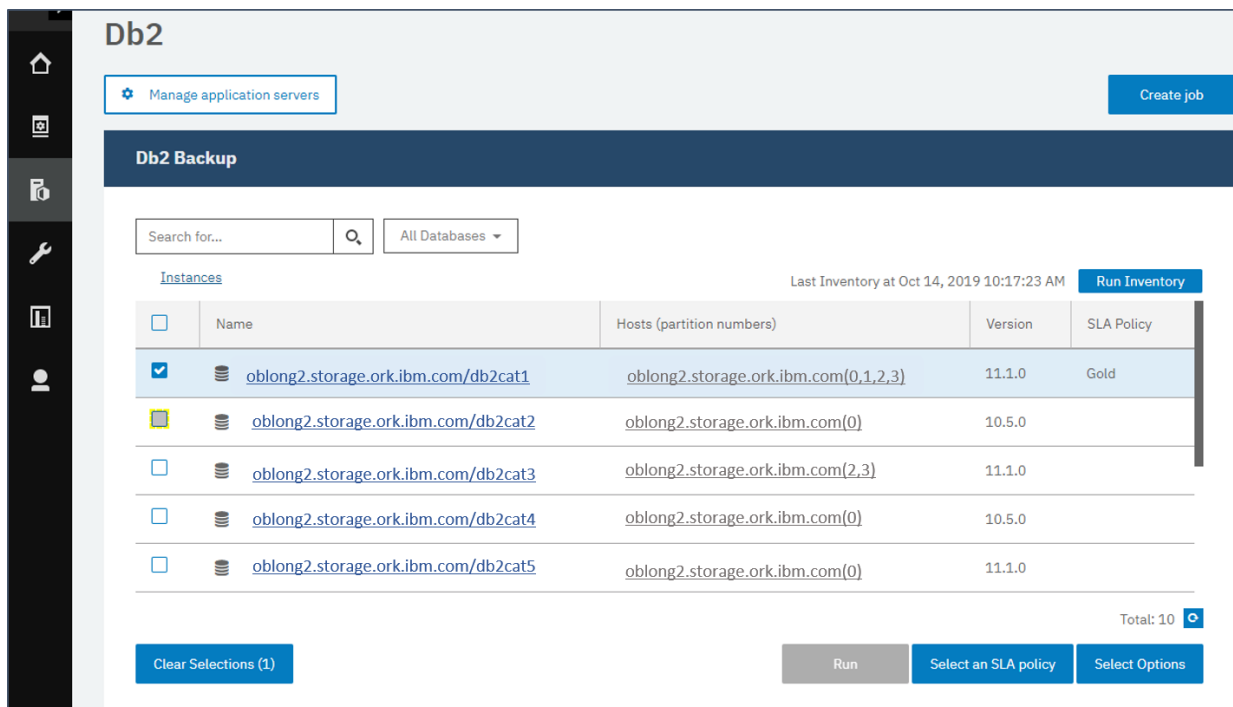


Figura 39. Detectando recursos do Db2

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 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 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 SLA, consulte [Definindo uma política de SLA](#).

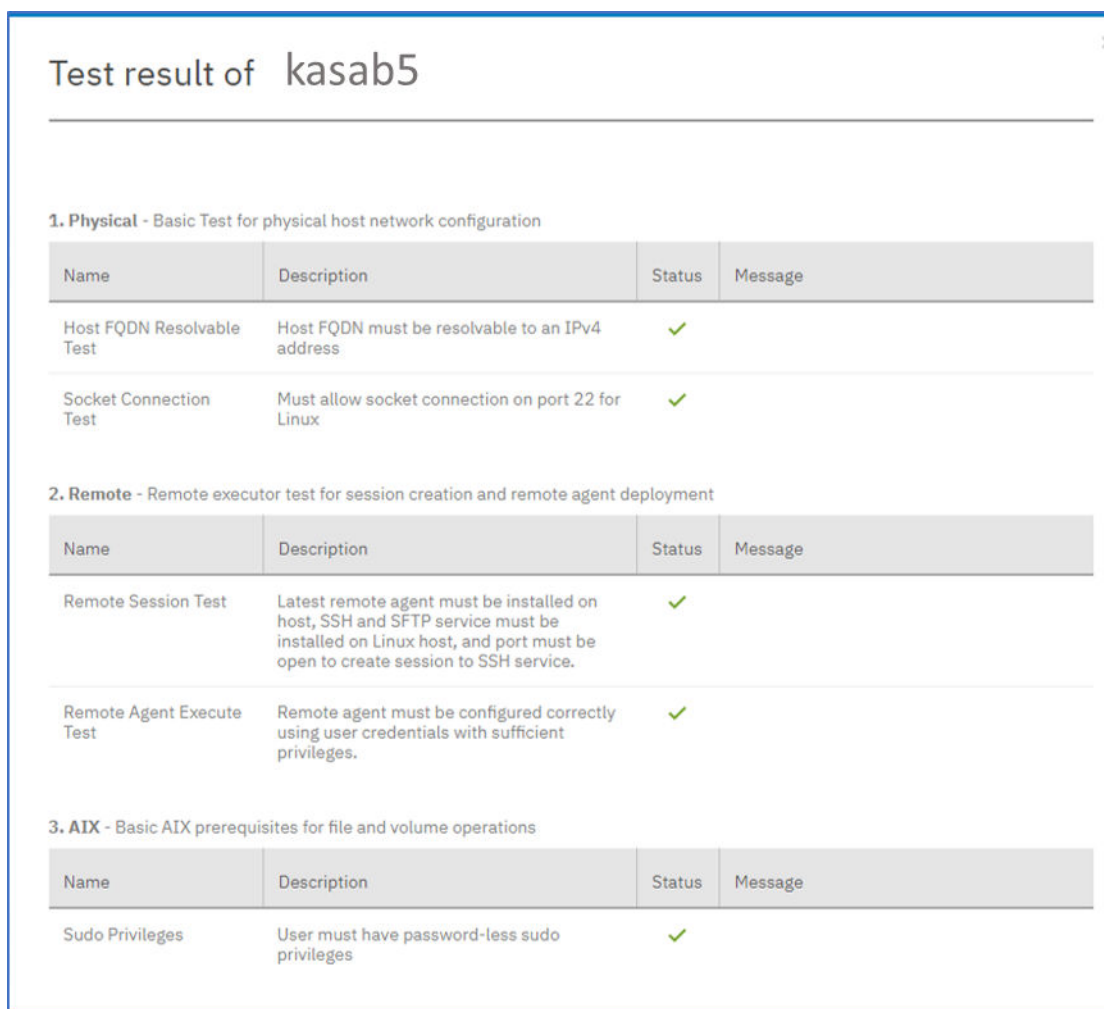
Testando a conexão Db2

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 40. 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, consulte [Capítulo 18, “Gerenciando o acesso de”, na página 517](#).
- 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.

Sobre Esta Tarefa

As etapas a seguir descrevem como fazer backup de recursos que são designados a uma política de SLA. Para executar uma tarefa de backup on demand para um ou mais recursos independentemente de esses recursos já estarem associados a uma política de SLA, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc” na página 503](#).

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar proteção > Aplicativos > Db2**.
2. Selecione um recurso para fazer backup.
 - Selecione uma instância inteira na área de janela **Instâncias** clicando na caixa de seleção 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.
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](#).

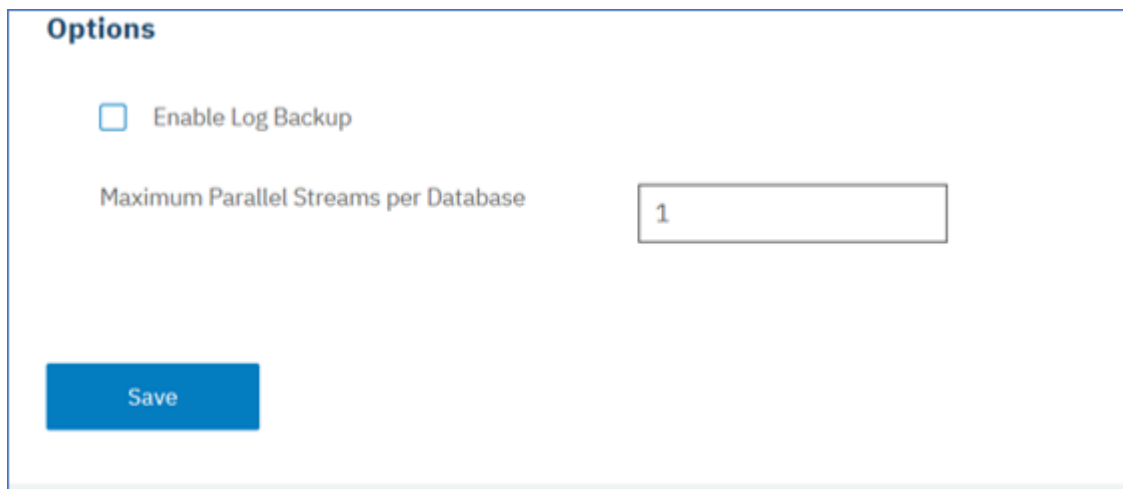


Figura 41. Área de janela Backup com a opção Ativar backup do log

Se uma tarefa on demand for executada com a opção **Ativar backup do log** ativada, o backup do log ocorrerá. No entanto, quando a tarefa é executada novamente em um planejamento, a opção é desativada para essa execução de tarefa para evitar possíveis segmentos ausentes na cadeia de backups.

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 SLA**, clique em **Incluir política de SLA** e defina suas preferências de política.

O que Fazer Depois

Quando a política de SLA é salva, você escolhe executar um backup on demand a qualquer momento clicando em **Ações** para essa 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 (SLA) 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.
- É possível fazer backup de uma instância inteira com todos os seus dados associados, ou fazer backup de um ou mais bancos de dados.

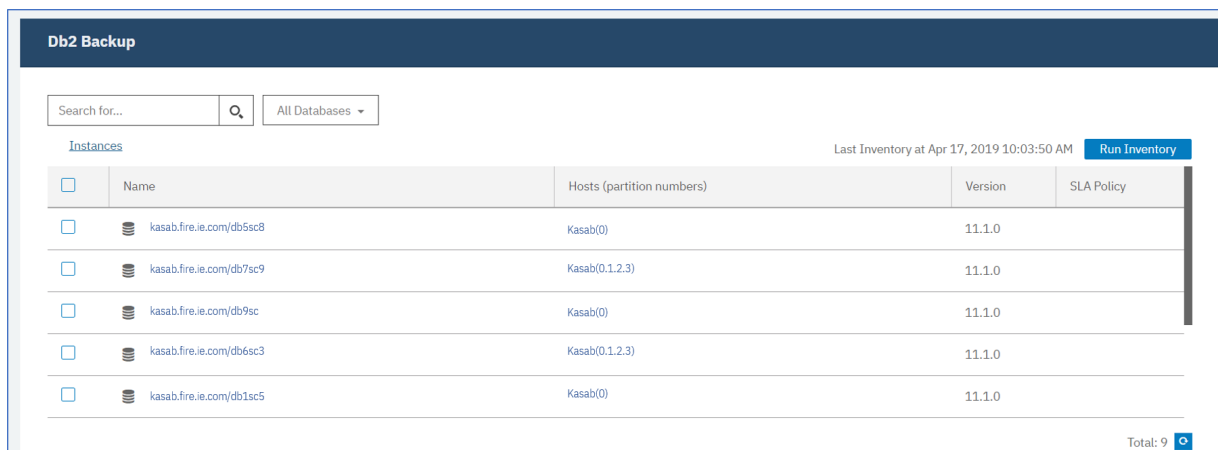


Figura 42. Área de janela de backup do Db2 mostrando instâncias

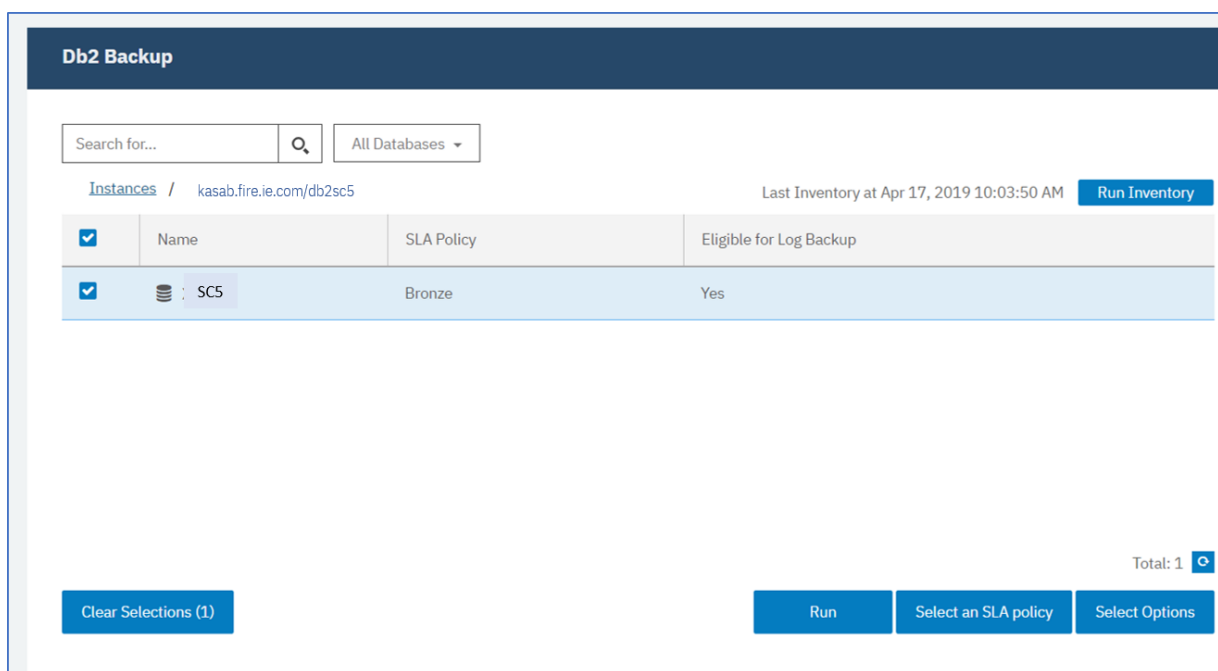


Figura 43. Área de janela Backup do Db2 que mostra bancos de dados em uma instância

3. Clique em **Selecionar Política de SLA** e selecione uma política SLA: **Gold**, **Silver** ou **Bronze**. Salve sua opção.

As políticas Gold, Silver e Bronze predefinidas têm frequências e taxas de retenção diferentes. É possível criar uma política de SLA customizada ou editar uma política existente navegando para **Visão Geral de Política > Políticas de SLA**.

4. Clique em **Selecionar Opções** para definir opções para o seu backup, como ativar backups de log para futuras opções de recuperação, e especificar os fluxos paralelos para reduzir o tempo necessário para fazer backup de grandes bancos de dados. Salve suas mudanças.

SLA Policy Status								
					Filter Job Log:	INFO ✕ WARN ✕ ERROR ✕ SUMMARY ✕		
Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	
> 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 PM	IDLE		Actions ▾
								Total: 4
Auto Refresh								

Figura 44. Opções de Backup e Políticas de SLA

- Configure a política de SLA clicando no ícone na coluna **Opções de política** da tabela **Status de política de SLA**.

Para ler sobre mais opções de configuração de SLA, consulte [“Configurando opções de configuração de SLA para uma tarefa de backup”](#) na página 375.

- Para 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 SLA escolhido e é possível acompanhar o progresso da tarefa no log da tarefa mostrado.

SLA Policy Status								
					Filter Job Log:	INFO ✕ WARN ✕ ERROR ✕ SUMMARY ✕		
Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	
> 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		Start Pause Schedule
> Gold	Every 4 Hours	0	0	0	Apr 23, 2019 2:05:00 PM	IDLE		Actions ▾
								Total: 4
Auto Refresh								

Figura 45. Políticas de SLA

Dica: Quando a tarefa para a política de SLA selecionada é executada, todos os recursos que estão associados a essa política de SLA são incluídos na operação de backup. Para fazer backup apenas de recursos selecionados, é possível executar uma tarefa on demand. Uma tarefa sob demanda executa a operação de backup imediatamente.

- Para executar uma tarefa de backup on demand para um único recurso, selecione o recurso e clique em **Executar**. Se o recurso não estiver associado a uma política de SLA, o botão **Executar** não estará disponível.
- Para executar uma tarefa de backup on demand para um ou mais recursos, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.

Para pausar o planejamento de um SLA, clique em **Ações** e escolha **Pausar planejamento**.


Para cancelar uma tarefa após ela ter sido iniciada, clique em **Ações** > **Cancelar**.

Configurando opções de configuração de SLA para uma tarefa de backup

Depois de configurar um acordo de nível de serviço, (SLA), 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 SLA** 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.

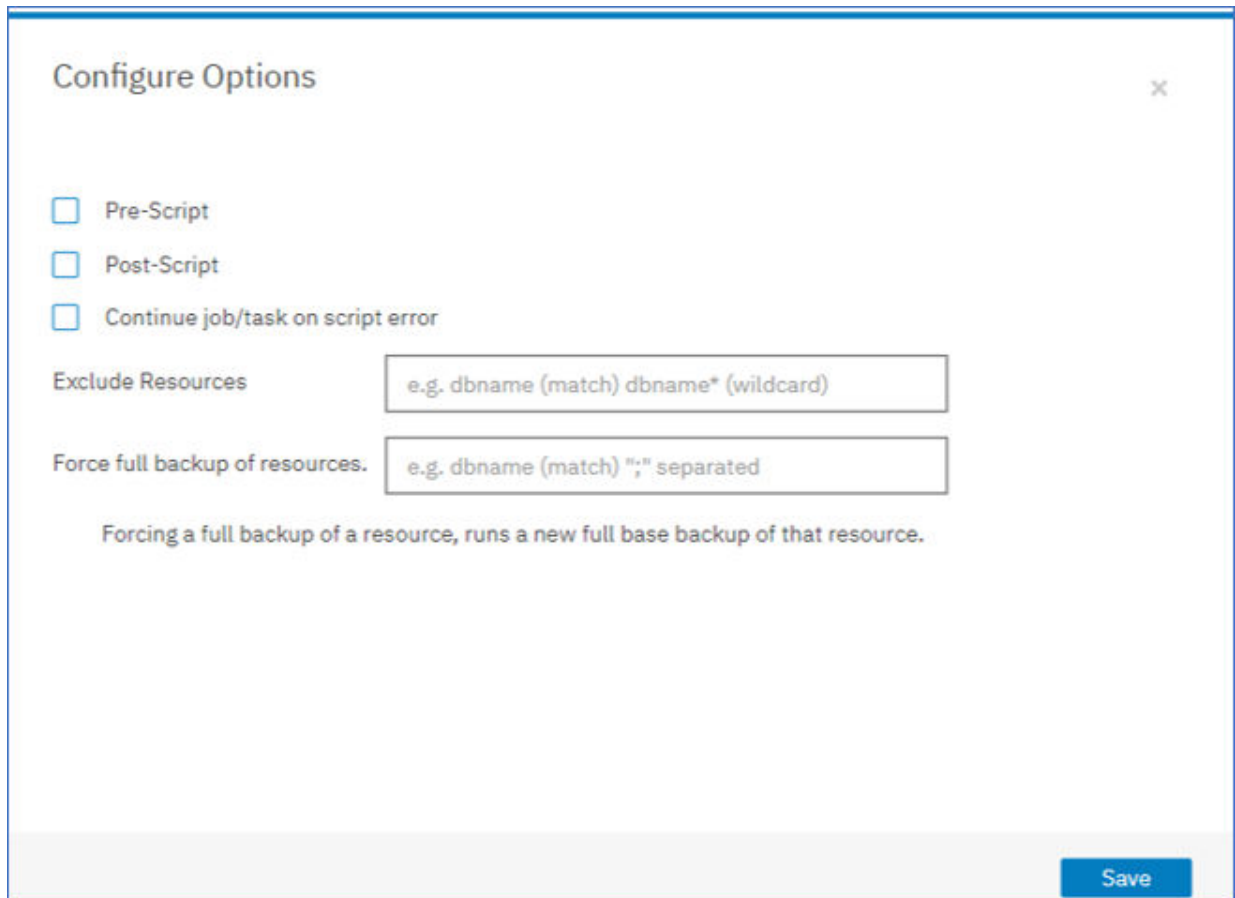


Figura 46. Especificando Opções de Configuração do SLA

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 372.](#)

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 370.](#)
- 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 18, “Gerenciando o acesso de”, na página 517.](#)
- 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 > Restaurar**.

O assistente Restauração é aberto.

2. Opcional: Se você iniciou o assistente de restauração a partir da página **Tarefas e Operações**, clique em **Db2** como o tipo de origem e clique em **Avançar**.

Dicas:

- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
3. Na página **Selecionar 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  para o nome desse 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: point-in-time:** cria uma operação de restauração única a partir de um backup point-in-time 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. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário

Opção	Descrição
	<p>de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>

Opção	Descrição
	<p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

6. 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](#).

7. 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.

8. 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**.

9. 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 Parallel 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.
10. 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.
 - **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.
11. 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.
12. 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.

13. 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 370](#).
- 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 18, “Gerenciando o acesso de”, na página 517](#).
- 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 > Restaurar**.

O assistente Restauração é aberto.

2. Opcional: Se você iniciou o assistente de restauração a partir da página **Tarefas e Operações**, clique em **Db2** como o tipo de origem e clique em **Avançar**.

Dicas:

- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
- O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.

3. Na página **Selecionar 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  para o nome desse 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: point-in-time:** cria uma operação de restauração única a partir de um backup point-in-time 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. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar. Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> • Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <p>Backup Restaura dados que são submetidos a backup para um servidor vSnap.</p> <p>Replicação Restaura dados que são replicados para um servidor vSnap.</p> <p>Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório.</p> <p>Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).</p> • Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.

Opção	Descrição
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>

Opção	Descrição
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 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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

6. 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.


7. 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.
8. Escolha as opções, conforme descrito em “Restaurando Dados do Db2 ” na página 377.
9. 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.

10. 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 370.
- 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 18, “Gerenciando o acesso de”,](#) na página 517.
- 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 > Restaurar**.
O assistente Restauração é aberto.
2. Opcional: Se você iniciou o assistente de restauração a partir da página **Tarefas e Operações**, clique em **Db2** como o tipo de origem e clique em **Avançar**.

Dicas:

- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
3. Na página **Selecionar 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  para o nome desse 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: point-in-time:** cria uma operação de restauração única a partir de um backup point-in-time 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. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar. Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> • Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <p>Backup Restaura dados que são submetidos a backup para um servidor vSnap.</p> <p>Replicação Restaura dados que são replicados para um servidor vSnap.</p> <p>Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório.</p> <p>Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).</p>

Opção	Descrição
	<ul style="list-style-type: none"> Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p>


Opção	Descrição
	Secundário O site secundário por meio do qual restaurar capturas instantâneas. 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 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	Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

6. 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.
7. 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.
8. Escolha as opções, conforme descrito em [“Restaurando Dados do Db2 ” na página 377](#).
9. Na página **Planejamento**, nomeia 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.
10. 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**.

Exchange Server

Depois de registrar com sucesso um servidor de aplicativos Exchange, é possível começar a proteger os dados do Microsoft Exchange com 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 Exchange Server

Certifique-se de que todos os pré-requisitos para o aplicativo Microsoft Exchange sejam atendidos antes de começar a proteger bancos de dados do Exchange com IBM Spectrum Protect Plus.

Para obter mais informações, consulte [“Microsoft Requisitos do Exchange Server”](#) na página 66.

Suporte de virtualização

O IBM Spectrum Protect Plus suporta o Exchange Server em execução em um servidor físico (bare metal), bem como em 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 garantir que um agente do Exchange possa trabalhar em seu ambiente IBM Spectrum Protect Plus, você deve configurar os privilégios apropriados para a conta do usuário do Exchange.

Controle de Acesso Baseado na Função

Você é obrigado a registrar o Exchange Server com IBM Spectrum Protect Plus com um usuário do Exchange que tenha privilégios de administrador local e as permissões corretas de controle de acesso baseado em função (RBAC).

Além disso, para operações de restauração granular, você é obrigado a usar um usuário do Exchange que tenha privilégios de administrador local e as permissões corretas do RBAC.

Para atender aos requisitos mínimos para um usuário do Exchange, conclua as etapas a seguir:

1. Verifique se o usuário do Exchange é um membro de um grupo de Administrador local e possui uma caixa de correio do Exchange ativa no domínio.

Por padrão, o Windows inclui o grupo Administradores da organização do Exchange em outros grupos de segurança, incluindo o grupo Administradores locais. Para usuários do Exchange que não são membros do grupo Gerenciamento da Organização do Exchange, deve-se incluir manualmente a conta do usuário no grupo de Administradores locais, tomando uma das ações a seguir:

- No computador do membro de domínio, clique em **Ferramentas Administrativas > Gerenciamento de Computador > Ferramenta de Usuários e Grupos Locais**.
- Em um computador de controlador de domínio que não tem um grupo de Administradores local ou ferramenta de Usuários e Grupos Locais, inclua manualmente a conta do usuário no grupo de Administradores no domínio: clique em **Ferramentas Administrativas > Ferramenta de Usuários e Computadores do Active Directory**.

2. Configure a função e o escopo.

- Verifique se o usuário do Exchange possui as permissões de RBAC corretas.

Você deve designar as seguintes funções de gerenciamento para cada usuário do Exchange que concluirá as operações de restauração de caixa postal:

- 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

Coloque os usuários que completam tarefas de restauração de caixa postal em um grupo de funções do Exchange Server que contém essas funções.

O Exchange Server inclui vários grupos de funções integrados. O grupo de funções de Gerenciamento da Organização, por padrão, contém a maioria das, se não todas as, funções que estão listadas.

Coloque os usuários que devem concluir várias tarefas de restauração de caixa de correio no grupo de funções de Gerenciamento da Organização (garantindo que o grupo contenha todas as funções listadas).

Como alternativa, é possível colocar o usuário em outro grupo de funções que você criou ou qualquer outro grupo de funções integrado que contém as funções listadas. Um usuário cujo nome não esteja no grupo de funções de Gerenciamento de Organização ou subgrupos poderá experimentar um desempenho mais lento durante as operações de restauração.

Importante: É possível gerenciar grupos de funções do Exchange usando o Exchange Admin Center (EAC) ou o Exchange Powershell Cmdlets *apenas* se o seu nome de usuário for autorizado pela política de segurança em sua organização.

- Escopo de 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

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.

Certificados do Exchange

Os certificados digitais do Exchange devem estar instalados e configurados para que o navegador da caixa de correio funcione durante uma operação de restauração granular. Certifique-se de que os certificados atuais do Exchange estejam instalados e configurados corretamente em seu ambiente.

Nota: Com o Exchange 2016 e o Exchange 2019, o Exchange Server é configurado para usar a Segurança da Camada de Transporte (TLS) por padrão. Esta segurança do TLS criptografa a comunicação entre servidores Exchange internos e entre os serviços do Exchange no servidor local.

Incluindo um servidor de aplicativos do Exchange

Quando você registra o Exchange Server, um inventário de bancos de dados do Exchange é incluído no IBM Spectrum Protect Plus. Quando o inventário estiver disponível, é possível começar a fazer backup e restaurar os bancos de dados do Exchange e executar relatórios.

Sobre Esta Tarefa

Para registrar um servidor de aplicativos Exchange, é necessário o endereço IP ou o nome do host.

Procedimento

Para incluir um servidor de aplicativos Exchange, conclua as etapas a seguir:

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Bancos de Dados > 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 391.
5. No campo **Máximo de Bancos de Dados Simultâneos**, configure o número máximo de bancos de dados por política de acordo de nível de serviço (SLA) que podem ser submetidos a backup simultaneamente. O padrão é 10. Os valores válidos são 1 - 99.

Esse valor pode ser maior ou menor do que o número de bancos de dados que estão associados a uma política de SLA. Por exemplo, se uma política de SLA tiver dez bancos de dados associados e esse valor for configurado para 2, uma operação de backup ocorrerá para apenas dois dos dez bancos de dados ao mesmo tempo. À medida que cada operação de backup é concluída, uma segunda operação de backup começa até que seja concluído o backup de todos os bancos de dados. Se uma política de SLA tiver cinco bancos de dados associados e esse valor for configurado para dez, todas as cinco operações de backup de banco de dados ocorrerão ao mesmo tempo.

Essa opção se aplica apenas a políticas de SLA que estão associadas a diversos bancos de dados. Para políticas de SLA que estão associadas a apenas um banco de dados, essa opção não fornece nenhuma função.

O número máximo de operações de backup de banco de dados simultâneas é limitado pelo seu ambiente. Algumas coisas a serem consideradas são a configuração do servidor vSnap, a largura de banda da rede e a configuração de disco físico do seu servidor IBM Spectrum Protect Plus.

Para obter orientação sobre o ajuste do seu ambiente IBM Spectrum Protect Plus para melhor desempenho, consulte o [Blueprints do IBM Spectrum Protect Plus](#).

6. Clique em **Salvar** e repita as etapas para incluir outras instâncias do Microsoft Exchange no IBM Spectrum Protect Plus.

Importante: Em um ambiente de grupo de disponibilidade do banco de dados (DAG), registre todos os servidores de aplicativos do 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 bancos de dados do Exchange executando um inventário”](#) na página 394. 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 395.

Detectando bancos de dados do Exchange executando um inventário

Ao incluir suas instâncias do 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 servidor de aplicativos do Exchange” na página 393](#).

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Bancos de Dados > 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 o servidor de aplicativos 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 do 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 > Bancos de Dados > 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 do Exchange

Para proteger bancos de dados do 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

Assegure-se de que os servidores de aplicativos que contiverem os bancos de dados do Exchange dos quais você deseja fazer backup estejam registrados com o IBM Spectrum Protect Plus. Para obter mais informações, consulte [“Incluindo um servidor de aplicativos do Exchange”](#) na página 393.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Bancos de Dados > 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 inicia e é possível visualizar os detalhes em **Tarefas e operações > Executando tarefas**.
Dica: O botão **Executar** é ativado somente para um backup de banco de dados único e o banco de dados deve ter uma política de SLA aplicada.
Para executar uma tarefa de backup on demand para vários bancos de dados que estão associados a uma política de SLA, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.
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 395.

Definindo uma tarefa de backup de Acordo de Nível de Serviço

Quando seus bancos de dados do Exchange são listados para cada uma de suas instâncias do Exchange Server, selecione e aplique uma política de acordo de nível de serviço (SLA) para iniciar a proteção de seus dados.

Sobre Esta Tarefa

IBM Spectrum Protect Plus suporta bancos de dados únicos ou múltiplos do Exchange 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 > Bancos de Dados > 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 SLA customizada ou editar uma política existente. Para obter mais informações, consulte [“Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos”](#) na página 236.
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 SLA clicando no ícone na coluna **Opções de política** da tabela **Status de política de SLA**.

Para obter informações adicionais sobre opções de configuração de SLA, consulte [“Configurando opções de configuração de SLA para uma tarefa de backup”](#) na página 396.

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 SLA 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 SLA para uma tarefa de backup

Depois de configurar um acordo de nível de serviço, (SLA), para sua tarefa de backup, é possível optar por configurar mais opções para essa tarefa. As opções extras de SLA 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 SLA** 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 do Exchange

É possível fazer backup dos logs de transações do banco de dados para bancos de dados 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 SLA.

Procedimento

1. Na área de janela de navegação, expanda **Gerenciar Proteção > Bancos de Dados > Exchange**.
2. Clique na instância do Exchange Server que você deseja proteger e, em seguida, selecione os bancos 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**.
Se uma tarefa on demand for executada com a opção **Ativar backup do log** ativada, o backup do log ocorrerá. No entanto, quando a tarefa é executada novamente em um planejamento, a opção é desativada para essa execução de tarefa para evitar possíveis segmentos ausentes na cadeia de backups.
4. **Restrição:** Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.
Insira a frequência dos backups de log em **Minutos, Horas, Dias, Semanas, Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.
5. Escolha o **Horário de Início**, selecione o horário para os backups de log começarem e 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 Exchange Server por 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 Exchange Database Availability Group (DAG) e especificar se deve-se usar 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 um 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 > Bancos de Dados > 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 Exchange DAG 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 SLA selecionadas e as opções do nó preferencial.
7. Para executar a política selecionada fora do planejamento, na área de janela **Status da política de SLA**, 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.
3. 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 bancos de dados do Exchange

Se os dados em um banco de dados do Exchange forem perdidos ou corrompidos, será possível restaurar os dados por meio de uma cópia de backup. Use o assistente **Restauração** para configurar um planejamento de tarefas 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 Exchange é 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 395.
- 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 18, “Gerenciando o acesso de”](#), na página 517.
- 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 login 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 do 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 do Exchange para a instância original

Restaure um banco de dados do 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 Exchange é 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 18, “Gerenciando o acesso de”](#), na página 517.

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 > Bancos de Dados > Exchange > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Exchange**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
2. Na página **Selecionar origem**, tome as ações 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado para um recurso em nuvem ou um servidor do repositório, um servidor</p>

Opção	Descrição
	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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Ponto de Restauração	Para operações de restauração sob demanda, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de data selecionado.

Opção	Descrição
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

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 de recuperação usando os arquivos de dados diretamente do repositório 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 você escolhe restauração de Produção, mas isso é para restaurar para um novo local de banco de dados na instância original. Para obter instruções detalhadas sobre esta tarefa, consulte [“Restaurando um banco de dados do Exchange para um novo local na instância original” na página 403](#).

6. Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
7. 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.

8. 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.
9. 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**.
10. 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 do Exchange para um novo local na instância original

É possível restaurar um banco de dados do 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 > Bancos de Dados > Exchange > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Exchange**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
2. Na página **Selecionar origem**, tome as ações 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none">• Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir:<ul style="list-style-type: none">Backup Restaura dados que são submetidos a backup para um servidor vSnap.Replicação Restaura dados que são replicados para um servidor vSnap.Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório.Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).• Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.

Opção	Descrição
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</p> <p>Se você estiver restaurando dados de um servidor de nuvem ou de repositório, selecione um servidor no menu Selecionar uma localização.</p>

Opção	Descrição
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 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	Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

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.

- 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.
- No campo **Novo nome do banco de dados**, insira o novo nome para o banco de dados restaurado.
- No campo **Caminho de Destino**, insira o novo local do diretório para o arquivo do banco de dados no servidor, incluindo o nome .edb e o local dos logs.



Aviso: Os diretórios de destino que você inserir no campo **Caminho de Destino** já devem existir no host de aplicativos. Se não, crie os diretórios necessários no servidor antes de concluir a operação de restauração.

Por exemplo, para um banco de dados denominado Database_A, insira

C:\<new_destination_path>\Database_A.edb, e para o local dos logs, insira C:\<new_logs_path>.

- Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
- 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 Parallel 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.

8. 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.
9. 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**.
10. 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 do 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 > Bancos de Dados > Exchange > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Exchange**.
- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.

- O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
- Na página **Selecionar origem**, tome as ações a seguir:
 - 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**.
 - 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.
 - Clique em **Avançar** para continuar.
 - Na página **Captura instantânea de origem**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

- Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.
Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> • Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <p>Backup Restaura dados que são submetidos a backup para um servidor vSnap.</p> <p>Replicação Restaura dados que são replicados para um servidor vSnap.</p> <p>Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório.</p>

Opção	Descrição
	<p>Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).</p> <ul style="list-style-type: none"> Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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>

Opção	Descrição
	Primário O site primário por meio do qual restaurar capturas instantâneas. Secundário O site secundário por meio do qual restaurar capturas instantâneas. 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 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	Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

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 de recuperação usando os arquivos de dados diretamente do repositório 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) (Restaurar somente produção) Expanda o nome do banco de dados para ver as informações dos caminhos de origem e de destino. No campo **Caminho de Destino**, insira o local do diretório do arquivo de banco de dados do Exchange no host alternativo, incluindo o nome .edb e o local de logs.



Aviso: Os diretórios de destino que você inserir no campo **Caminho de Destino** já devem existir no host alternativo. Se não, crie os diretórios necessários no host alternativo antes de concluir a operação de restauração.

Por exemplo, para um banco de dados denominado Database_A, insira
C:\<new_destination_path>\Database_A.edb, e para o local dos logs, insira c:\<new_logs_path>.

6. 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**.
7. 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.

8. 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.
9. 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**.
10. 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 os itens da caixa de correio individual do Exchange usando uma operação de restauração granular e a GUI do IBM Spectrum Protect Plus Microsoft Management Console (MMC).

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 391), ou executar o assistente de configuração do IBM Spectrum Protect Plus para configurar permissões automaticamente (consulte a etapa “15” na página 415).

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 > Bancos de Dados > Exchange > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Exchange**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no</p>

Opção	Descrição
	servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

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. Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
7. 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.
8. 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.
9. 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**.
10. 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**.
11. 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.
12. 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 login 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**.
13. Na GUI do MMC do IBM Spectrum Protect Plus, clique no nó **Proteger e recuperar dados** e selecione **Exchange Server**.
14. 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.
15. 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**.
16. 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.

Tabela 62. Visualizando e filtrando itens de caixa de correio	
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>

17. 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.

18. 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 63. 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 63. 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>

19. 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>).

20. Quando a operação de restauração para os itens individuais for concluída, retorne para IBM Spectrum Protect Plus. Na área de janela **Tarefas e Operações > Recursos Ativos**, clique em **Ações > Cancelar Restauração Granular** para encerrar o processo de restauração granular.

Restaurando caixas de correio usando uma operação de restauração granular

É possível restaurar caixas de correio do 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 391), ou executar o assistente de configuração do IBM Spectrum Protect Plus para configurar permissões automaticamente (consulte a etapa “15” na página 422).

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 > Bancos de Dados > Exchange > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Exchange**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.


Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none">• Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).• Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

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. Na página **Configurar destino**, selecione **Restaurar para instância original** e clique em **Avançar**.
7. 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.
8. 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.
9. 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**.
10. 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**.
11. 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.
12. 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 login 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**.
13. Na GUI do MMC do IBM Spectrum Protect Plus, clique no nó **Proteger e recuperar dados** e selecione **Exchange Server**.
14. 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.
15. 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**.
16. 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, Aliás, 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.

17. Para concluir a operação de restauração, na área de janela **Ações**, clique em uma das seguintes opções de restauração.

Tabela 64. Opções de Restauração	
Opção	Ação
Restaurar Correio para Local Original	Restaure os itens de correio para seu local no momento da operação de backup.
Restaurar Correio para Local Alternativo	<p>Restaure os itens de correio para uma caixa de correio diferente.</p> <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. 	<p>Restaure itens de correio para um arquivo de pastas pessoais não Unicode (.pst).</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. Cada caixa de correio é restaurada para um arquivo .pst separado que reflete o nome da caixa de correio no diretório especificado.</p> <p>Se o arquivo .pst já existir, o arquivo será usado. Caso contrário, o arquivo será criado.</p>

Tabela 64. Opções de Restauração (continuação)

Opção	Ação
Restaurar Correio para o Arquivo PST Unicode	<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>
Restaurar Caixa de Correio de Pasta Pública	<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 64. 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>).

- 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 > Bancos de Dados > Exchange > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Exchange**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:

Opção	Descrição
	<ul style="list-style-type: none"> Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>

Opção	Descrição
	<p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

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. 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.

7. 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 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.

8. 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.
9. 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**.
10. 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 do banco de dados do Exchange usando o tipo de restauração de acesso instantâneo e montar os arquivos do banco de dados 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 > Bancos de Dados > Exchange > Criar Tarefa** e, em seguida, selecione **Restauração** para abrir o assistente **Restauração**.

Dicas:


- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Exchange**.
- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
- O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.

2. Na página **Selecionar origem**, tome as ações 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> • Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). • Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p>

Opção	Descrição
	<p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

5. 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.

Opção	Descrição
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.

- Na página **Método de restauração**, escolha **Acesso instantâneo** e, em seguida, clique em **Avançar**.
- Opcional: Na página **Opções da tarefa**, configure as opções adicionais, se necessário e clique em **Avançar** para continuar.
- 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.
- 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**.
- 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**.
- 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.
- 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 72.

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.

- Certifique-se de que tenha atendido aos requisitos de espaço, conforme descrito em [Requisitos de espaço para proteção do MongoDB](#).
- 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 arquivos maiores 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.
- 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 72. Para obter informações sobre como configurar privilégios sudo, consulte [“Configurando Privilégios Sudo”](#) na página 436.

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 434.
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.

A button with a blue background, a white plus icon, and the text "Add application server".

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.

MongoDB

Manage application servers

Create job

Manage application servers

Application Properties

Host Address: metali.ca.ibm.com

User (selected) | SSH Key

Use existing user: ☒

Select user: sppagent_metal.ca.ibm.com

Get Instances

Name	Status	Configured
------	--------	------------

Figura 47. 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 18, “Gerenciando o acesso de”](#), na página 517.

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](#).

Registrando um MongoDB Ops Manager Application Database para proteção

Para proteger seu MongoDB Ops Manager Application Database, primeiro você deve registrar o endereço do host do Ops Manager com IBM Spectrum Protect Plus.

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**.



3. No formulário Propriedades do Aplicativo, insira o endereço do host para o Ops Manager Application Database. Obtenha as instâncias e configure as credenciais seguindo as etapas descritas em [“Incluindo um servidor de aplicativos MongoDB” na página 436](#).

O Ops Manager Application Database é listado na tabela Instâncias, conforme mostrado no exemplo a seguir:

```
metali8.limerick.ie.ibm.com Connection: '333.0.5.1:88888' Ops Manager Application Database
```

O que Fazer Depois

O MongoDB Ops Manager Application Database está disponível para backup. É possível definir tarefas de backup e restauração 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 (SLA). Para obter mais informações, consulte [“Fazendo backup de dados do MongoDB” na página 440](#) e [“Definindo uma tarefa de acordo de nível de serviço regular” na página 442](#).

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

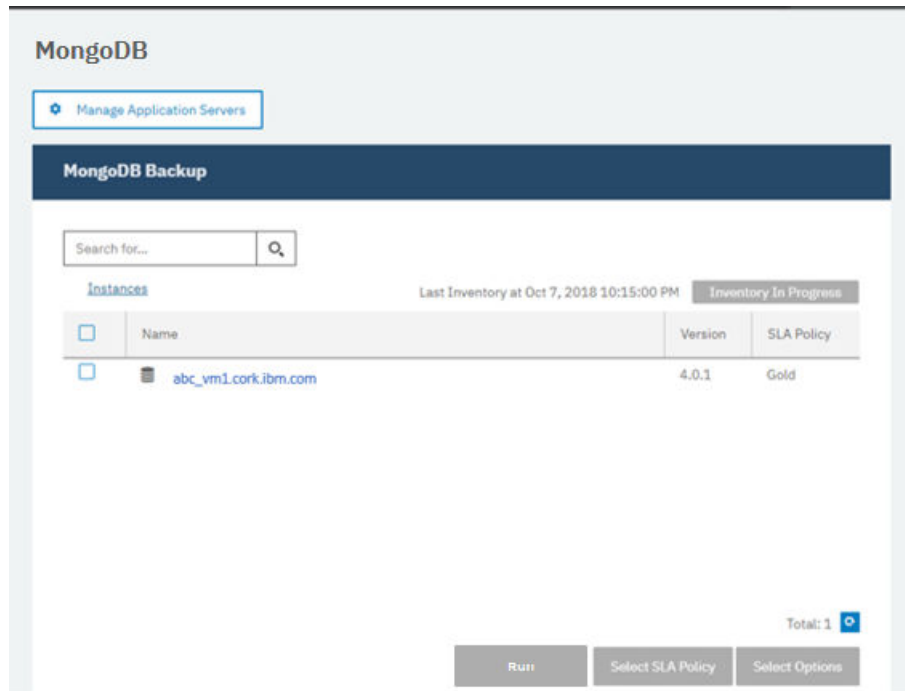
Certifique-se de que tenha incluído servidores de aplicativos MongoDB no IBM Spectrum Protect Plus. Para obter instruções, consulte [Incluindo um servidor de aplicativos MongoDB](#).

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 (SLA) à instância. Para obter instruções sobre como configurar uma política de SLA, consulte [Definindo uma política de SLA](#).

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

É possível definir tarefas de backup para proteger seus dados do MongoDB. Para fazer backup de seus dados regularmente, defina uma tarefa de backup que inclua uma política de acordo de nível de serviço (SLA).

Antes de Iniciar

Durante a operação de backup inicial, o IBM Spectrum Protect Plus cria um volume de vSnap e compartilhamento 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 18, “Gerenciando o acesso de”, na página 517](#) e [“Roles para MongoDB” na página 434](#).

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 SLA 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 inicia e é possível visualizar os detalhes em **Tarefas e operações > Executando tarefas**.

Dica: O botão **Executar** é ativado apenas se uma política de SLA é aplicada à representação **ALL** dos bancos de dados.

Para executar uma tarefa de backup on demand para vários bancos de dados que estão associados a uma política de SLA, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc” na página 503](#).

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 SLA 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 SLA**, clique em **Incluir política de SLA** e defina preferências de política.

O que Fazer Depois

Depois que a política de SLA é salva, é possível executar a política a qualquer momento clicando em **Ações** para esse nome de 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** para esse nome de 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 SLA 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.

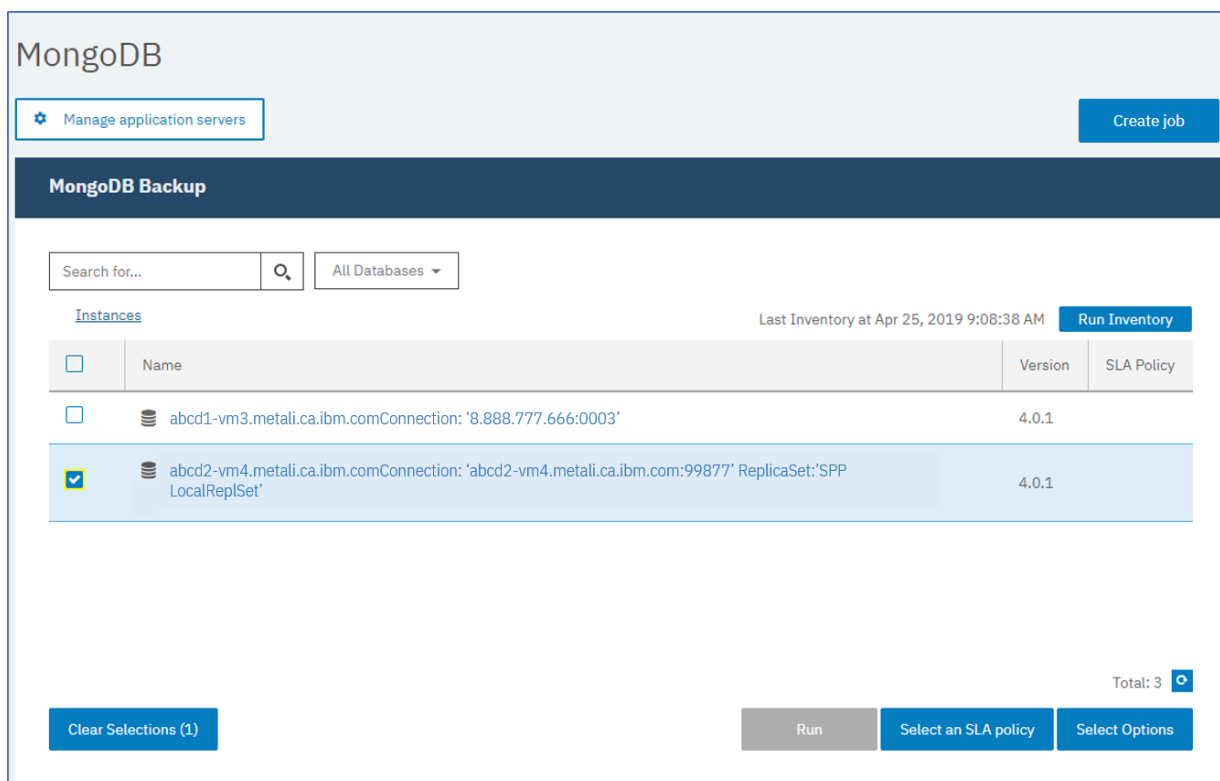


Figura 48. Área de Janela de Backup MongoDB mostrando instâncias

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 SLA customizada navegando para **Visão geral de política > Incluir política de SLA**.

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.

Options

Maximum Parallel Streams per Database:

SLA Policy Status

Filter Job Log: Info x Warning x Error x Summary x

Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	
> Gold	Every 4 Hours	1	1	0	Apr 25, 2019 10:05:00 AM	Idle		Actions

Figura 49. Opções de backup e status da política de SLA

- Configure a política de SLA clicando no ícone na coluna **Opções de política** da tabela **Status de política de SLA**.

Para obter informações adicionais sobre opções de configuração de SLA, consulte [“Definindo opções de configuração de SLA para seu backup”](#) na página 443.

- 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 SLA escolhido e é possível acompanhar o progresso da tarefa no log mostrado.

O que Fazer Depois


Depois que a política de SLA é salva, é possível executar a política a qualquer momento clicando em **Ações** para esse nome de 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** para esse nome de 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 SLA para seu backup

Depois de configurar uma política de acordo de nível de serviço (SLA) para sua tarefa de backup, é possível escolher configurar opções extras para essa tarefa. As opções adicionais de SLA incluem executar scripts e forçar um backup de base completo.

Procedimento

- Na coluna **Opções de política** da tabela **Status da política de SLA** 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 50. 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 SLA 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 440.
- 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 18, “Gerenciando o acesso de”](#), na página 517 e [“Roles para MongoDB”](#) na página 434.
- 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**, em seguida, selecione **Restaurar** para abrir o assistente de Restauração.

Dicas:

- Você também pode abrir o assistente clicando em **Trabalhos e Operações > Criar Tarefa > Restauração > MongoDB**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
2. Na página **Selecionar origem**, tome as ações 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none">• Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).• Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo	Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap

Opção	Descrição
para a tarefa de restauração	<p>alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.

Opção	Descrição
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

- 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.

- 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](#).

- 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.

8. 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.

9. Na página **Planejar**, clique em **Avançar** para iniciar tarefas on demand após concluir o assistente de Restauração. Para tarefas recorrentes, insira um nome para o planejamento de tarefa e especifique com que frequência e quando iniciar a tarefa de restauração.
10. 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.

11. 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 440](#).
- 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 18, “Gerenciando o acesso de”, na página 517](#) e [“Roles para MongoDB” na página 434](#).
- 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**, em seguida, selecione **Restaurar** para abrir o assistente de Restauração.

Dicas:

- Você também pode abrir o assistente clicando em **Trabalhos e Operações > Criar Tarefa > Restauração > MongoDB**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
2. Na página **Selecionar origem**, tome as ações 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário

Opção	Descrição
	<p>de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p>

Opção	Descrição
	<p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

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. Na página **Configurar Destino**, escolha **Restaurar para a Instância Original** e clique em **Avançar**.

7. 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.

8. 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.

9. Na página **Planejar**, clique em **Avançar** para iniciar tarefas on demand após concluir o assistente de Restauração. Para tarefas recorrentes, insira um nome para o planejamento de tarefa e especifique com que frequência e quando iniciar a tarefa de restauração.
10. 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.

11. 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 440.
- 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 18, “Gerenciando o acesso de”,](#) na página 517 e [“Roles para MongoDB”](#) na página 434.
- 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**, em seguida, selecione **Restaurar** para abrir o assistente de Restauração.


Dicas:

- Você também pode abrir o assistente clicando em **Trabalhos e Operações > Criar Tarefa > Restauração > MongoDB**.
- Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
- O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.

2. Na página **Selecionar origem**, tome as ações 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> • Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). • Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p>

Opção	Descrição
	<p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

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. 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.

7. 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 Paralel 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.

8. 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.

9. Na página **Planejar**, clique em **Avançar** para iniciar tarefas on demand após concluir o assistente de Restauração. Para tarefas recorrentes, insira um nome para o planejamento de tarefa e especifique com que frequência e quando iniciar a tarefa de restauração.
10. 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.

11. 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 > Criar Tarefa**, em seguida, selecione **Restaurar** para abrir o assistente **Restaurar**.
2. Na página **Selecionar origem**, tome as ações 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 **Método de restauração**, selecione **Testar** e clique em **Avançar** para continuar com o processo de restauração de teste.
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. Prossiga pelas páginas do assistente de restauração e selecione as opções necessárias.
6. 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.

7. Efetue login no servidor MongoDB para o qual a tarefa de restauração de teste é direcionada.
8. Execute o comando do sistema `ps -ef | grep mongod` do MongoDB para encontrar o local da instância do MongoDB de recuperação temporária.
9. 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>
```

10. 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>
```

11. Quando a operação de restauração de banco de dados ou de coleta for concluída, acesse **Tarefas e operações > Recursos ativos**.
12. Clique em **Ações > Cancelar restauração** para terminar o procedimento de restauração granular.

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 de backup e restauração do banco de dados Oracle Server”](#) na página 82.

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 > Bancos de Dados > Oracle**.
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 do usuário e senha inseridos anteriormente para o servidor de aplicativos. Selecione um nome do usuário da lista Selecionar usuário.</p>

Opção	Descrição
	<p>UserID</p> <p>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</p> <p>Insira sua senha para o servidor de aplicativos.</p>
Chave SSH	Clique nesta opção para usar uma chave SSH. Selecione uma chave da lista Selecionar uma chave SSH .

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 **Save**. 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 523.

Conceitos relacionados

[“Gerenciando o acesso de”](#) na página 517

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 464

Use uma tarefa de backup para fazer backup de ambientes Oracle com capturas instantâneas.

[“Restaurando dados do Oracle” na página 467](#)

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 > Bancos de Dados > Oracle**.
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 Plus e o host.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Bancos de Dados > Oracle**.
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 18, “Gerenciando o acesso de”, na página 517](#).
- Registre os provedores dos quais você deseja fazer backup. Para obter mais informações, consulte [“Incluindo um servidor de aplicativos Oracle” na página 462](#).
- Configure políticas do SLA. Para obter mais informações, consulte [“Criar políticas de backup” na página 163](#).

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 a tarefa de backup é concluída, o agente IBM Spectrum Protect Plus desmonta o compartilhamento do servidor Oracle e cria 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 462](#).

Procedimento

Para definir uma tarefa de backup do Oracle, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Bancos de Dados > 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 de 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: Quando a tarefa para a política de SLA selecionada é executada, todos os recursos que estão associados a essa política de SLA são incluídos na operação de backup. Para fazer backup apenas de recursos selecionados, é possível executar uma tarefa on demand. Uma tarefa sob demanda executa a operação de backup imediatamente.

- Para executar uma tarefa de backup on demand para um único recurso, selecione o recurso e clique em **Executar**. Se o recurso não estiver associado a uma política de SLA, o botão **Executar** não estará disponível.
 - Para executar uma tarefa de backup on demand para um ou mais recursos, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc” na página 503](#).
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**.

Se uma tarefa on demand for executada com a opção **Ativar backup do log** ativada, o backup do log ocorrerá. No entanto, quando a tarefa é executada novamente em um planejamento, a opção é desativada para essa execução de tarefa para evitar possíveis segmentos ausentes na cadeia de backups.

A **Frequência** pode ser configurada como um valor independente da frequência de backup de banco de dados especificada nas configurações de Política de SLA. Por exemplo, a Política de SLA 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 SLA.

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 os 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 Paralel 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**.

7. Para configurar opções adicionais, clique no ícone de área de transferência **Opções de Política**  que está associado à tarefa na seção **Status de Política de SLA**. Configure as opções de política adicionais a seguir:

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.

Excluir Recursos

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 467.

Conceitos relacionados

[“Configurando scripts para operações de backup e restauração”](#) na página 504

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 464.
- 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 18, “Gerenciando o acesso de”, na página 517.

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 > Bancos de Dados > Oracle > Criar Tarefa**, em seguida, selecione **Restaurar** para abrir o assistente **Restaurar**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > Oracle**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
2. Na página **Selecionar origem**, tome as ações 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none">• Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita).• Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo .

Opção	Descrição
	Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
Ponto de Restauração	Para operações de restauração sob demanda, selecione uma captura instantânea na lista de capturas instantâneas disponíveis no intervalo de data selecionado.

Opção	Descrição
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

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 **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.

7. 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

Restaurar 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

Alterne 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.

8. 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.

9. 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**.

10. 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 504](#)

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 462](#)

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.

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 [“Requisitos de backup e restauração do banco de dados Microsoft SQL Server” na página 90](#).

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.

Todo host do Microsoft SQL Server pode usar uma conta de usuário específica para acessar os recursos dessa instância do SQL server 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: [Erro do Planejador de Tarefas "Uma sessão de logon especificada não existe"](#)

Incluindo um servidor de aplicativos SQL Server

Quando um servidor de aplicativos SQL Server 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 incluir um host do SQL Server, conclua as etapas a seguir.

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Bancos de Dados > SQL**.
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.

Password

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 523.

Conceitos relacionados

[“Gerenciando o acesso de”](#) na página 517

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 477

Use uma tarefa de backup para fazer backup de ambientes SQL Server com capturas instantâneas.

[“Restaurando os Dados do SQL Server”](#) na página 481

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 > Bancos de Dados > SQL**.
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 Plus e o host.

Procedimento

Para testar a conexão, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Gerenciar Proteção > Bancos de Dados > SQL**.
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 volume de LUN vSnap e cria um compartilhamento NTFS nesse LUN iSCSI. Durante backups incrementais, o volume criado anteriormente é reutilizado. O agente IBM Spectrum Protect Plus mapeia o LUN para o servidor SQL Server e monta o volume NTFS para onde o backup é concluído. Se os backups de log estiverem ativados, o IBM Spectrum Protect Plus cria um volume de vSnap separado e cria um CIFS nesse volume. Os arquivos de transação de backup do log são copiados para esse compartilhamento de acordo com o planejamento criado para backup de log.

Quando a tarefa de backup é concluída, o agente IBM Spectrum Protect Plus desmonta o compartilhamento do servidor SQL Server e cria uma captura instantânea 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 18, “Gerenciando o acesso de”, na página 517](#).
- 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 informações adicionais, consulte [Microsoft iSCSI Initiator Step-by-Step Guide](#).
- O IBM Spectrum Protect Plus não suporta o backup do log de modelos de recuperação simples.

- 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](#).
- O IBM Spectrum Protect Plus suporta backups de banco de dados e backups do log de transações. O nome do produto é preenchido no msdb . dbo . backupset para registros criados por backups iniciados a partir de IBM Spectrum Protect Plus.
- Para obter mais informações sobre backups de log para SQL, consulte [“Backups de log”](#) na página 480.

Nota: Devido a limitações com a estrutura de Serviços de Cópia de Sombra de Volume (VSS), espaços iniciais, espaços finais e caracteres não imprimíveis não devem ser usados em nomes de banco de dados. Para obter mais informações, consulte <https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa>

Execute as seguintes ações:

- Registre os Servidores SQL do quais você deseja fazer backup. Para obter mais informações, consulte [“Incluindo um servidor de aplicativos SQL Server”](#) na página 475.
- Configure políticas do SLA. Para obter mais informações, consulte [“Criar políticas de backup”](#) na página 163.
- Antes de configurar e executar tarefas de backup SQL, configure as definições de armazenamento de Cópia de Sombra para os volumes em que os bancos de dados SQL estão localizados. Essa definição é configurada uma vez para cada volume. Se novos bancos de dados forem incluídos na tarefa, a configuração deverá ser configurada para quaisquer novos volumes que contenham bancos de dados SQL. No Windows Explorer, clique com o botão direito do mouse no volume de origem e selecione a guia **Cópias de Sombra**. Configure o **Tamanho máximo** para **Nenhum limite** ou um tamanho razoável com base no tamanho do volume de origem e nas atividades de E/S e, em seguida, clique em **OK**. A área de armazenamento de cópia de sombra deve estar em um mesmo volume ou outro volume disponível durante a tarefa 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 > Bancos de Dados > 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 de 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: Quando a tarefa para a política de SLA selecionada é executada, todos os recursos que estão associados a essa política de SLA são incluídos na operação de backup. Para fazer backup apenas de

recursos selecionados, é possível executar uma tarefa on demand. Uma tarefa sob demanda executa a operação de backup imediatamente.

- Para executar uma tarefa de backup on demand para um único recurso, selecione o recurso e clique em **Executar**. Se o recurso não estiver associado a uma política de SLA, o botão **Executar** não estará disponível.
- Para executar uma tarefa de backup on demand para um ou mais recursos, clique em **Criar Tarefa**, selecione **Backup Ad Hoc** e siga as instruções em [“Executando uma tarefa de backup ad hoc”](#) na página 503.

5. Clique em **Selecionar Opções** para especificar mais opções antes de salvar a tarefa de backup.

Ativar Backup de Log

Selecione esta opção para ativar o backup de logs de transações. Esses logs são usados para opções de recuperação, tais como operações de restauração de point-in-time. Se os backups de log estiverem ativados para suas tarefas de backup, as transações serão registradas continuamente durante o tempo de backup. A notificação é enviada se alguma descontinuidade for detectada em backups de arquivo de log.

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 SLA. Uma área temporária para o processo de backup do log não é necessária.

Se uma tarefa on demand for executada com a opção **Ativar backup do log** ativada, o backup do log ocorrerá. No entanto, quando a tarefa é executada novamente em um planejamento, a opção é desativada para essa execução de tarefa para evitar possíveis segmentos ausentes na cadeia de backups.

Selecione uma das seguintes opções:


Fazer backup de um arquivo de banco de dados por vez usando fluxos paralelos Selecione esta opção para usar fluxos paralelos para fazer backup de seus bancos de dados sequencialmente.

Fazer backup de arquivos de banco de dados em paralelo usando fluxos paralelos Selecione esta opção para usar fluxos paralelos para fazer backup de seus bancos de dados em paralelo.

Por fim, configure o **Máximo de Fluxos Paralelos por Banco de Dados**, selecionando o número máximo de fluxos de dados a serem usados por banco de dados durante o processo 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 for configurado como **1**. A especificação de diversos fluxos paralelos pode melhorar a velocidade de backup em alguns casos.

6. Clique em **Salvar** para salvar as opções para suas tarefas de backup.

A tarefa é executada conforme definido pela sua política de SLA, ou pode ser executada manualmente a partir da janela **Tarefa e Operações**.

7. Para configurar opções adicionais, clique no ícone de área de transferência **Opções de Política**  que está associado à tarefa na seção **Status de Política de SLA**. Configure as opções de política adicionais a seguir:

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 aplicativo ou script no qual o script deve ser executado. Para selecionar um servidor de aplicativos no qual o script é 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 essa opção estiver ativada, se um pré-script ou pós-script finalizar o processamento com um código de retorno diferente de zero, a operação de backup ou restauração será tentada e o status da tarefa de pré-script será relatado como COMPLETED. Se um pós-script for concluído com um código de retorno diferente de zero, o status da tarefa pós-script será relatado como COMPLETED.

Quando essa opção não é ativada, o backup ou restauração não é tentado e o status da tarefa de pré-script ou pós-script é relatado como FAILED.

Excluir Recursos

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, além dos caracteres especiais a seguir: - _ 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 481 .

Conceitos relacionados

“Configurando scripts para operações de backup e restauração” na página 504

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 sob demanda” na página 497

É possível executar qualquer tarefa on demand, mesmo que a tarefa esteja configurada para ser executada em um planejamento.

Backups de log

Os arquivos de log arquivados para bancos de dados contêm dados de transações confirmados. Esses dados de transação podem ser usados para executar um processo de rollforward de recuperação como parte de 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 que os backups de log estejam ativados em suas tarefas de backup para permitir o rollforward de recuperação quando você restaurar os dados do Microsoft SQL Server.

Ao ativar backups de log pela primeira vez, deve-se executar uma tarefa de backup para a política de SLA para ativar o arquivamento de log para o IBM Spectrum Protect Plus no banco de dados. Esse backup cria um volume separado no repositório vSnap e o volume é montado persistentemente no servidor de aplicativos SQL. O volume permanece montado no servidor de aplicativos SQL, a menos que a opção

Ativar Backup de Log esteja limpa e uma nova tarefa de backup seja executada. Para ativar backups de log, siga as instruções em [“Fazendo Backup dos Dados do SQL Server” na página 477](#).

Revise os critérios a seguir antes de configurar operações de backup de log:

- Para executar backups de log, o usuário do agente do SQL Server deve ser um administrador local do Windows. Esse usuário deve ter permissão sysadmin para gerenciar tarefas do agente do SQL Server. O agente usa essa conta do administrador para ativar e acessar tarefas de backup de log. Para cada instância do SQL Server, o usuário do agente do SQL Server também deve ser o usuário do serviço SQL Server e a conta de serviço do agente do SQL Server. Essa regra é verdadeira para cada instância do SQL Server a ser protegida.
- O IBM Spectrum Protect Plus não suporta operações de backup de log para modelos de recuperação simples.
- Evite configurar backups de log para um único banco de dados SQL usando várias tarefas de backup. Os logs são truncados durante as operações de backup de log. Se um único banco de dados SQL for incluído em várias definições de tarefa com backup de log ativado, um backup de log de uma tarefa truncará um log antes que a próxima tarefa faça seu backup. Essa sobreposição pode fazer com que as tarefas de restauração de momento falhem.
- Antes de os logs serem copiados para o repositório do vSnap, IBM Spectrum Protect Plus usa a pasta de backup que é configurada para a instância do SQL Server como a área temporária para coletar logs. O volume em que esta pasta está localizada deve ter espaço suficiente para conter os logs de transações entre as tarefas de backup. A área temporária pode ser modificada, alterando a configuração da pasta de backup no SQL Server Management Studio (SSMS).
- O IBM Spectrum Protect Plus suporta backups de banco de dados e backups do log de transações. O nome do produto é preenchido no msdb . dbo . backupset para registros que são criados por backups iniciados a partir de IBM Spectrum Protect Plus.
- 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 IBM Spectrum Protect Plus, os logs não serão truncados e devem ser gerenciados separadamente.
- Quando uma tarefa de backup SQL é concluída com backups de log ativados, todos os logs de transações até a conclusão dessa tarefa são limpos do SQL Server. A limpeza de log ocorre apenas se a tarefa de backup do SQL for concluída com sucesso. Se os backups de log não forem submetidos a backup durante uma reprise da tarefa, a limpeza do log não ocorrerá.
- Uma operação de backup de log para um banco de dados secundário SQL Server Always On pode falhar com o seguinte erro:

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.

Se esse erro ocorrer, altere a preferência de backup do grupo de disponibilidade para `Principal`. Os logs são então submetidos a backup a partir da réplica primária. Depois que um backup de log bem-sucedido da réplica principal for concluído com sucesso, a preferência de backup poderá ser alterada.

- Se um banco de dados de origem for sobrescrito, todos os logs de transações anteriores até esse ponto serão colocados em um diretório *condense* depois que o banco de dados original for restaurado. Quando a próxima execução da tarefa de backup do SQL Server for concluída, o conteúdo da pasta condensada será removido.

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 477.

- 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 18, “Gerenciando o acesso de”, na página 517](#).
- 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 <https://docs.microsoft.com/en-us/sql/t-sql/language-reference?view=sql-server-2017>.

- 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 > Bancos de Dados > SQL**. Clique em **Criar Tarefa** e, em seguida, selecione **Restaurar** para abrir o assistente **Restaurar**.

Dicas:

- Você também pode abrir o assistente clicando em **Tarefas e Operações > Criar Tarefa > Restaurar > SQL**.
 - Para um resumo em execução de suas seleções no assistente, clique em **Visualizar restauração** na área de janela de navegação no assistente.
 - O assistente é aberto no modo de configuração padrão. Para executar o assistente no modo de configuração avançado, selecione **Configuração avançada**. Com o modo de configuração avançado, é possível configurar mais opções para a sua tarefa de restauração.
2. Na página **Selecionar origem**, tome 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**, selecione o tipo de tarefa de restauração que você deseja criar:

On-demand: captura instantânea

Executa uma operação de restauração única. 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.

4. Preencha os campos na página **Captura instantânea de origem** e clique em **Avançar** para continuar.

Os campos que são mostrados dependem do número de itens que foram selecionados na página **Selecionar origem** e no tipo de restauração. Alguns campos também não são mostrados até que você selecione um campo relacionado.

Campos que são mostrados para uma captura instantânea on demand, restauração de recurso único

Opção	Descrição
Intervalo de Data	Especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.

Opção	Descrição
Tipo de armazenamento de backup	<p>Todos os backups no intervalo de data selecionado são listados em linhas que mostram o horário em que ocorreu a operação de backup e a política de acordo de nível de serviço (SLA) para o backup. Selecione a linha que contém o horário de backup e a política de SLA que você deseja e, em seguida, tome uma das ações a seguir:</p> <ul style="list-style-type: none"> Clique no tipo de armazenamento de backup por meio do qual você deseja restaurar. Os tipos de armazenamento que são mostrados dependem dos tipos que estão disponíveis em seu ambiente e são mostrados na ordem a seguir: <ul style="list-style-type: none"> Backup Restaura dados que são submetidos a backup para um servidor vSnap. Replicação Restaura dados que são replicados para um servidor vSnap. Armazenamento de Objeto Restaura dados que são copiados para um serviço de nuvem ou para um servidor do repositório. Archive Restaura dados que são copiados para um archive de serviços de nuvem ou para um archive do servidor do repositório (fita). Clique em qualquer lugar na linha O primeiro tipo de backup que é mostrado sequencialmente por meio da esquerda da linha é selecionado por padrão. Por exemplo, se os tipos de armazenamento Backup, Replicação e Archive forem mostrados, o Backup será selecionado por padrão.
Usar servidor vSnap alternativo para a tarefa de restauração	<p>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione esta caixa para especificar um servidor vSnap alternativo e, em seguida, selecione um servidor no menu Selecionar vSnap alternativo.</p> <p>Quando você restaurar dados por meio de um ponto de restauração que foi copiado 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

Campos que são mostrados para uma captura instantânea on demand, restauração de recursos múltiplos; restauração point-in-time; ou restauração recorrente

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 para o qual as capturas instantâneas foram submetidas a backup. O site é definido na área de janela Configuração do sistema > Site.</p> <p>Serviço em nuvem O serviço de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p>

Opção	Descrição
	<p>Servidor de repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas. O servidor do repositório é definido na área de janela Configuração do sistema > Armazenamento de backup > Servidor do repositório.</p> <p>Archive de serviços de nuvem O serviço de archive de nuvem para o qual as capturas instantâneas foram copiadas. O serviço de nuvem é definido na área de janela Configuração do sistema > Armazenamento de backup > Armazenamento de objeto.</p> <p>Archive do servidor do repositório O servidor do repositório para o qual as capturas instantâneas foram copiadas para fita. 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 site primário por meio do qual restaurar capturas instantâneas.</p> <p>Secundário O site secundário por meio do qual restaurar capturas instantâneas.</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 on demand, especifique um intervalo de datas para mostrar as capturas instantâneas disponíveis dentro desse intervalo.
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>Se você estiver restaurando dados de um serviço de nuvem ou de um servidor do repositório, selecione 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 copiado para um serviço de nuvem ou servidor do 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 cópia. Para reduzir a carga no servidor vSnap, é possível selecionar um servidor vSnap alternativo para servir como o gateway.</p>

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.

Opcionalmente, para restauração de Teste apenas, 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 você escolhe restauração de Produção, mas isso é para restaurar para um novo local de banco de dados na instância original. Ao renomear um banco de dados SQL, aplicam-se as regras de nomenclatura para identificadores. Para obter mais informações, consulte <https://docs.microsoft.com/en-us/sql/relational-databases/databases/database-identifiers>.

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 **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.

7. 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.

Modo de espera

Quando a opção de modo de espera é selecionada, isso deixa o banco de dados SQL em um estado somente leitura. As transações não confirmadas são desfeitas e salvas em um arquivo undo que pode ser usado posteriormente para deixar o banco de dados on-line. As transações armazenadas no arquivo de espera podem ser aplicadas quando o banco de dados estiver pronto para ser recuperado.

Nota: O local de um banco de dados restaurado usando o modo de Espera pode ser relatado como estando no local do banco de dados original ao visualizar o banco de dados no SQL Management Studio. O local será, na verdade, o diretório especificado pelo usuário para uma restauração de modo de Produção e o C:\ProgramData\mnt\uuid_subdirectory para uma restauração do modo de Teste.

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 Parallel 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

Alterne 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.

8. 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.

9. 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**.

10. 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 504

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 475

Quando um servidor de aplicativos SQL Server 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.

[“Fazendo Backup dos Dados do SQL Server”](#) na página 477

Use uma tarefa de backup para fazer backup de ambientes SQL Server com capturas instantâneas.

Capítulo 15. 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 e informações de tarefas são submetidas a backup em um servidor vSnap que é definido na política de SLA associada.

Fazendo backup do aplicativo IBM Spectrum Protect Plus

Faça backup de definições de configuração do IBM Spectrum Protect Plus, políticas de SLA, recursos registrados, configurações de armazenamento de backup, pontos de restauração e chaves importadas e certificados para um servidor vSnap que é definido na política de SLA associada.

Antes de Iniciar

Assegure-se de que uma política de SLA adequada esteja disponível. Para otimizar tarefas de backup, crie políticas de SLA especificamente para fazer backup do IBM Spectrum Protect Plus. Para reduzir a carga do sistema, assegure-se de que outras tarefas não estejam planejadas para execução durante a tarefa de backup do IBM Spectrum Protect Plus. Para criar uma política de SLA, siga as instruções em [“Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos”](#) na página 236.

Restrição: Não é possível selecionar o servidor vSnap integrado como o destino da política de SLA para 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 quando você criar a política de SLA para fazer backup de IBM Spectrum Protect Plus.

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 SLA para associar à operação de backup do catálogo do IBM Spectrum Protect Plus.
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 171.

Restaurando o aplicativo IBM Spectrum Protect Plus

Restaurar definições de configuração do IBM Spectrum Protect Plus, pontos de restauração e informações de tarefas 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 restaurar um backup em nuvem, o recurso em nuvem ou o servidor do repositório deve ser registrado no local alternativo do IBM Spectrum Protect Plus.

Quando uma tarefa de restauração do catálogo é iniciada, um identificador de sessão de tarefa (ID) é designado. Durante a fase inicial, a tarefa estará disponível para ser monitorada na UI do IBM Spectrum Protect Plus na tela de gerenciamento de tarefas, até que a etapa de recuperação inicie a restauração do banco de dados interno. Uma vez que a tarefa entra nesse estado, o IBM Spectrum Protect Plus não está mais disponível. Durante essa fase, as informações do log são gravadas no local: `/data/log/adminconsole/managedb-catalogrestore-time.log`, em que *time* é o horário de época. Os dados contidos nesse log estão relacionados com a restauração do catálogo de configuração e recuperação do mongo. Após o processo ser concluído, o virgo o serviço iniciará e os dados serão gravados no log do virgo. Quando a tarefa for concluída, a interface com o usuário do IBM Spectrum Protect Plus ficará acessível novamente.

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.

Conceitos relacionados

[“Tipos de Tarefa” na página 495](#)

As tarefas são usadas para executar operações de backup, restauração, manutenção, inventário e relatório em IBM Spectrum Protect Plus.

Expirando sessões de tarefa

Você pode expirar uma sessão de tarefa para substituir as configurações de retenção de capturas instantâneas que foram designadas durante a criação do backup.


Sobre Esta Tarefa

Expirar uma sessão de tarefa não removerá uma captura instantânea e um ponto de recuperação relacionado se a captura instantânea for bloqueada por um relacionamento de replicação ou cópia. Execute a tarefa ativada por replicação ou cópia para alterar o bloqueio para uma captura instantânea posterior. 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 ponto de restauração. Como alternativa, na guia Máquinas Virtuais/Bancos de Dados, selecione Aplicativos ou Hypervisores para procurar a entrada do catálogo desejada inserindo o nome. Os nomes podem ser procurados inserindo texto parcial usando o asterisco (*) como um caractere curinga ou usando o ponto de interrogação (?) para correspondência de padrões.

Para obter informações adicionais sobre como usar a função de procura, consulte [Apêndice A, “Diretrizes de Procura”](#), na página 551.
3. Se você estiver procurando na guia Sessões de Backup, use filtros para ajustar sua procura aos tipos de tarefa e intervalo de data quando a tarefa de backup associada foi iniciada.
4. Clique no ícone procurar .
5. Selecione as sessões de tarefa 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**.

Excluindo metadados de recursos do catálogo IBM Spectrum Protect Plus

Quando você executa uma tarefa de inventário, os recursos são incluídos no catálogo IBM Spectrum Protect Plus. Para liberar espaço no catálogo, é possível expirar os metadados dos pontos de restauração que estão associados com os recursos.



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 551.
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 que estão associados ao recurso são removidos do catálogo.

Conceitos relacionados

[“Tipos de Tarefa” na página 495](#)

As tarefas são usadas para executar operações de backup, restauração, manutenção, inventário e relatório em IBM Spectrum Protect Plus.

Capítulo 16. Gerenciando tarefas e operações

É possível gerenciar e monitorar tarefas na janela **Tarefas e Operações**. Também é possível configurar scripts para serem executados antes ou depois de tarefas.

Tipos de Tarefa

As tarefas são usadas para executar operações de backup, restauração, manutenção, inventário e relatório em 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, de inventário e de relatório são predefinidas e não modificáveis. No entanto, é possível modificar os planejamentos de tarefas de manutenção, inventário e relatório.

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.

Também é possível executar tarefas de backup para um único recurso ou vários recursos selecionados que estão associados a uma política de SLA em vez de fazer backup de todos os recursos que estão associados à política.

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.

As tarefas de restauração são executados em um planejamento ou on demand.

Para tarefas planejadas, o nome da tarefa é definido pelo usuário que cria a tarefa.

Para tarefas on demand, o nome da tarefa `onDemandRestore` é gerado automaticamente quando a tarefa é executada.

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.

Relatar

Uma tarefa de relatório executa um relatório planejado. O nome da tarefa é o nome do relatório precedido por Report_.

Os nomes de relatórios são semelhantes ao exemplo a seguir:

```
Report_VM Backup History
```

Conceitos relacionados

[“Protegendo sistemas virtualizados” na página 249](#)

Você deve registrar os sistemas virtualizados que deseja proteger em IBM Spectrum Protect Plus e, em seguida, criar tarefas para fazer backup e restaurar os recursos que estão associados aos sistemas.

[“Protegendo bancos de dados” na página 363](#)

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.

Tarefas relacionadas

[“Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos” na página 236](#)

Você pode criar políticas de acordo de nível de serviço (SLA) customizadas para definir as políticas de frequência de backup, retenção, replicação e cópia que são específicas para o seu ambiente.

[“Executando uma tarefa de backup ad hoc” na página 503](#)

Com uma tarefa de backup ad hoc, é possível selecionar um ou mais recursos que estão associados a uma política de SLA e executar uma operação de backup on demand para esses recursos.

Criando tarefas e programações de tarefas

O método para criação de tarefas e planejamentos de tarefas depende do tipo de tarefa.

É possível criar tarefas e planejamentos para tarefas de backup e restauração. A tabela a seguir descreve as tarefas de backup e restauração disponíveis e fornece links para as etapas que são necessárias para criar as tarefas e os planejamentos de tarefas ou executar as tarefas on demand.

As tarefas de manutenção são criadas por padrão. As tarefas de inventário e de relatório são criadas automaticamente quando uma operação de inventário é executada ou quando um relatório é planejado.

Tipo de Tarefa	Descrição	Como criar a tarefa
Backup	É possível criar uma definição de tarefa e designar uma ou mais políticas de acordo de nível de serviço (SLA) para essa definição. A definição de tarefa define os recursos para fazer backup e a política de SLA define o planejamento, as metas e outras opções para a operação de backup.	<p>Consulte os tópicos que contêm instruções para fazer backup de dados por tipo de recurso nas seções a seguir:</p> <ul style="list-style-type: none">• Capítulo 10, “Protegendo sistemas virtualizados”, na página 249• Capítulo 11, “Protegendo sistemas de arquivos”, na página 299• Capítulo 12, “Protegendo os contêineres”, na página 317• Capítulo 13, “Proteger dados em sistemas em nuvem”, na página 357• Capítulo 14, “Protegendo bancos de dados”, na página 363 <p>Por exemplo, o tópico de backup para VMware é “Fazendo backup dos dados de VMware” na página 253.</p>

Tipo de Tarefa	Descrição	Como criar a tarefa
Backup ad hoc	Quando uma tarefa é executada para a política de SLA selecionada, todos os recursos que estão associados a essa política de SLA são incluídos na operação de backup. Se você deseja fazer backup apenas de recursos selecionados usando uma política de SLA selecionada, é possível executar uma tarefa ad hoc, que executa a operação de backup imediatamente.	Consulte “Executando uma tarefa de backup ad hoc” na página 503.
Restaurar	Depois de ter executado um trabalho de backup pelo menos uma vez, é possível executar uma tarefa de restauração para restaurar os dados. É possível criar uma tarefa de restauração que é executada em um planejamento ou que é executada on demand.	Consulte os tópicos que contêm instruções para restauração de dados por tipo de recurso nas seções a seguir: <ul style="list-style-type: none"> • Capítulo 10, “Protegendo sistemas virtualizados”, na página 249 • Capítulo 11, “Protegendo sistemas de arquivos”, na página 299 • Capítulo 12, “Protegendo os contêineres”, na página 317 • Capítulo 13, “Proteger dados em sistemas em nuvem”, na página 357 • Capítulo 14, “Protegendo bancos de dados”, na página 363 Por exemplo, o tópico de restauração para VMware é “Restaurando Dados do VMware” na página 264.

Conceitos relacionados

[“Tipos de Tarefa”](#) na página 495

As tarefas são usadas para executar operações de backup, restauração, manutenção, inventário e relatório em IBM Spectrum Protect Plus.

Tarefas relacionadas

[“Criando uma política de SLA para hypervisors, bancos de dados e sistemas de arquivos”](#) na página 236


Você pode criar políticas de acordo de nível de serviço (SLA) customizadas para definir as políticas de frequência de backup, retenção, replicação e cópia que são específicas para o seu ambiente.

Iniciando tarefas sob demanda

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 você deseja executar, clique no ícone do menu de ações  e, em seguida, clique em **Iniciar**.
A tarefa é iniciada e incluída na guia **Tarefas em execução**.

O que Fazer Depois

Para visualizar o log de tarefas para a tarefa, selecione a tarefa na guia **Tarefas em execução** e clique em **Log de tarefas**. Para fazer o download do log para a tarefa, clique em **Download.zip**.

Para visualizar todas as tarefas que estão em execução ou que foram executadas simultaneamente com a tarefa, clique em **Tarefas Simultâneas**.

Visualizando Tarefas

Visualize informações sobre o status de suas tarefas em execução e o status geral das tarefas que são concluídas com sucesso ou com falhas ou avisos.

Procedimento

Para visualizar tarefas, conclua as seguintes etapas:

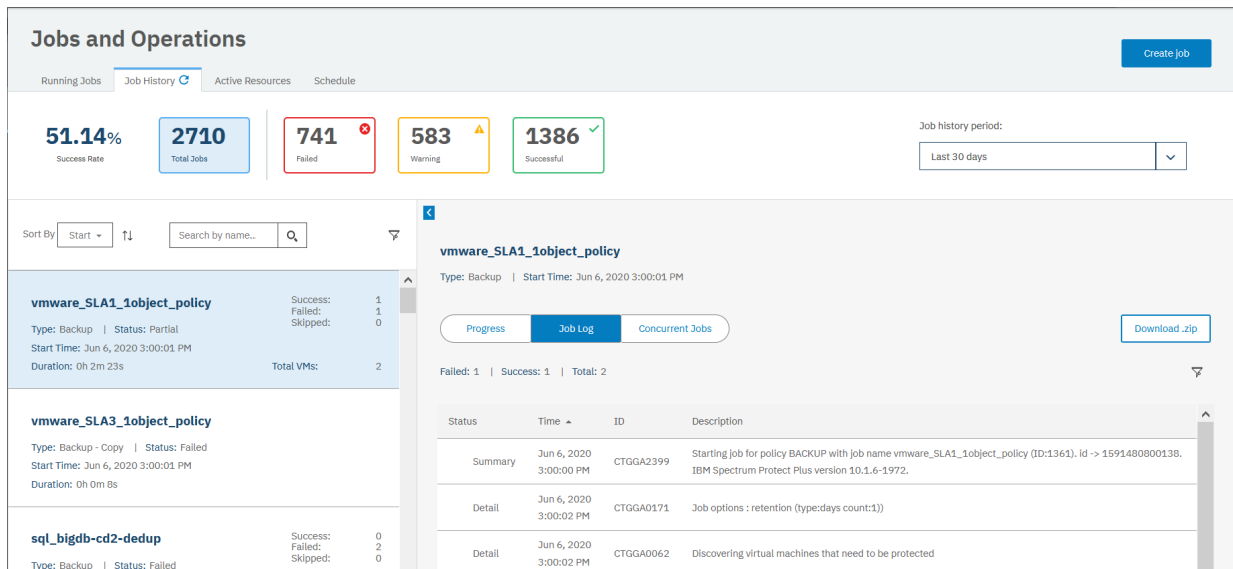
1. Na área de janela de navegação, clique em **Tarefas e operações**.
2. Na página **Tarefas em Execução**, visualize o status das tarefas que estão em execução atualmente, conforme mostrado no exemplo a seguir.

The screenshot displays the 'Jobs and Operations' interface. At the top, there's a navigation bar with tabs: 'Running Jobs' (selected), 'Job History', 'Active Resources', and 'Schedule'. Below this, a summary section shows counts for various job types: 7 Total Jobs, 0 Backup, 0 Inventory, 0 Maintenance, and 7 Restore. A 'CPU Usage' indicator shows 4% usage for the 'IBM Spectrum Protect Plus Host Machine'. The main content area is divided into two panels. The left panel lists jobs, with the first one selected: 'onDemandRestore_1590032799201'. This job is an SQL Restore, started on May 20, 2020, at 8:46:40 PM, with a duration of 0h 7m 24s. The right panel provides a detailed view of this job, showing its status as 'Restore' and 'Resource active'. It includes a 'Job Log' section with a table of job logs.

Status	Time	ID	Description
Summary	May 20, 2020 8:46:40 PM	CTGGA2398	Starting job for policy onDemandRestore_1590032799201 (ID:1654). id -> 1590032800093. IBM Spectrum Protect Plus version 10.1.6-1948.
Detail	May 20, 2020 8:46:41 PM	CTGGA2109	Policy has (1) destination database mappings.
Detail	May 20, 2020 8:46:41 PM	CTGGA1527	Resolved policy to (restore).

3. Para visualizar tarefas concluídas, clique em **Histórico de Tarefas**.

A faixa de opções nessa tela mostra o status de tarefas históricas. Use o filtro para definir a duração do histórico de tarefa a ser exibido.



4. Para visualizar os recursos ativos em seu ambiente, clique em **Recursos Ativos**.

Mostra recursos ativos de aplicativo e hypervisor. Para os hypervisors, os campos exibidos são recurso, tipo, destino e última atualização. As informações do rótulo do vDisk também serão exibidas se a origem do destino for um vDisk.

5. Para visualizar o planejamento geral para todas as tarefas, clique em **Planejar**.

Usando o menu **Ações**, é possível optar por iniciar uma tarefa ou pausar um planejamento. Também é possível editar alguns planejamentos de tarefas recorrentes e de manutenção clicando no ícone de planejamento e salvando suas mudanças. Para editar uma tarefa de restauração, clique no ícone de edição para essa tarefa.

6. Opcional: Para fazer download de um log de tarefas e outros arquivos que refletem as informações que são mostradas na janela **Tarefas e Operações**, clique em **Download.zip**.

Visualizando o progresso da tarefa de backup no nível de recursos

Visualize o status dos recursos individuais em uma tarefa de backup. A visualização da tarefa no nível de recurso permite que você determine o desempenho de backup de cada recurso. Esse recurso fornece informações para ajudá-lo a otimizar o desempenho de backup e resolver possíveis problemas.

Sobre Esta Tarefa

Esse recurso está disponível apenas para tarefas de backup. O progresso dos recursos individuais não é mostrado para outros tipos de tarefa.


Procedimento

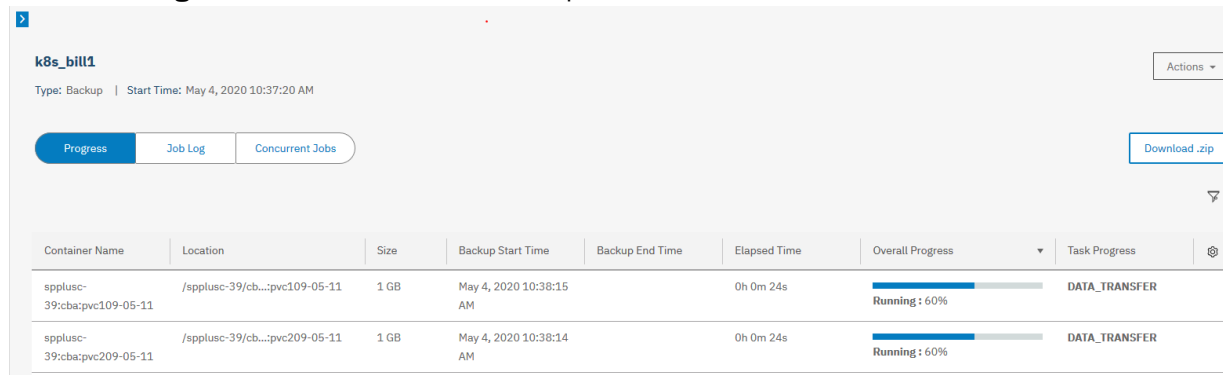
Para visualizar o progresso dos recursos individuais em uma tarefa de backup, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Tarefas e operações**.
2. Clique em **Tarefas em execução** para tarefas que estão em andamento ou em **Histórico de tarefa** para tarefas que estão concluídas.
3. Selecione a tarefa que contém os recursos que você deseja visualizar e, em seguida, clique em **Progresso**.

As informações sobre cada recurso são mostradas em uma tabela. Essas informações incluem o progresso da operação de backup para cada recurso na coluna **Progresso Geral**.

Se aplicável para o tipo de recurso, a tarefa que está em execução para a operação de backup também será mostrada na coluna **Progresso da Tarefa**. Essa coluna não está incluída para alguns tipos de recursos, como hypervisors, cujas operações de backup não incluem tarefas individuais.


O exemplo a seguir mostra as informações de progresso para uma tarefa de backup de Kubernetes. Neste exemplo, o progresso do backup geral para o recurso é 60%, conforme mostrado na coluna **Progresso Geral**. A tarefa de backup atual que está em execução, transferência de dados, é mostrada na coluna **Progresso da Tarefa**. A tabela foi expandida clicando na seta .




Container Name	Location	Size	Backup Start Time	Backup End Time	Elapsed Time	Overall Progress	Task Progress
spplusc-39:cbapvc109-05-11	/spplusc-39/cb...:pvc109-05-11	1 GB	May 4, 2020 10:38:15 AM		0h 0m 24s	Running : 60%	DATA_TRANSFER
spplusc-39:cbapvc209-05-11	/spplusc-39/cb...:pvc209-05-11	1 GB	May 4, 2020 10:38:14 AM		0h 0m 24s	Running : 60%	DATA_TRANSFER

Figura 51. Visualizando informações de tarefa no nível de recurso

4. Opcional: É possível customizar as colunas que são mostradas na tabela e filtrar os recursos que são mostrados pelo status do progresso.

Para customizar as colunas, clique no ícone de configurações  para selecionar as colunas. Por padrão, todas as colunas são mostradas.

Para filtrar os recursos por status de progresso, clique no ícone do filtro  e selecione os valores de status que você deseja. Por exemplo, se você deseja ver apenas recursos que estão em processo de execução, marque a caixa de seleção **Em Execução** e limpe as outras.

Visualizar Logs de Tarefa

Para cada tarefa executada, é fornecido um log que mostra tais informações, como o status da tarefa, o horário de início e de encerramento da tarefa e uma mensagem que está associada à tarefa.

Procedimento

Para visualizar logs de tarefas, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Tarefas e operações**
2. Clique em **Tarefas em execução** para tarefas que estão em andamento ou em **Histórico de tarefa** para tarefas que estão concluídas.
3. Selecione uma tarefa e clique em **Log de tarefas**.

O log da tarefa para a tarefa selecionada é mostrado.

Visualizando tarefas simultâneas

Tarefas que sobrepõem outras são chamadas de tarefas simultâneas. É possível visualizar tarefas que estão em execução ou que foram executadas simultaneamente com outra tarefa.

Procedimento

Para visualizar tarefas, que estão em execução ou que foram executadas simultaneamente com outra tarefa, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Tarefas e operações**
2. Clique em **Tarefas em execução** para tarefas que estão em andamento ou em **Histórico de tarefa** para tarefas que estão concluídas.
3. Selecione uma tarefa e clique em **Tarefas Simultâneas**.

Para tarefas que são mostradas na guia **Tarefas em Execução**, é mostrada uma lista de todas as tarefas que estão em execução simultaneamente com a tarefa selecionada. Para tarefas que são mostradas na guia **Histórico da Tarefa**, é mostrada uma lista de todas as tarefas que foram executadas simultaneamente com a tarefa selecionada.



Restrição: Tarefas de backup múltiplas não podem fazer backup do mesmo recurso ao mesmo tempo. Se várias tarefas compartilharem um recurso ou recursos, a tarefa que processar o recurso primeiro será executada e quaisquer outras tarefas que iniciarem durante o mesmo período de tempo falharão.

Pausando e Continuando Tarefas

É possível pausar e retomar uma tarefa planejada. 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 no ícone do menu de ações  e, em seguida, clique em **Pausar Planejamento**.
3. Para retomar o planejamento da tarefa, clique em  e, em seguida, clique em **Liberar Planejamento**.

Editando tarefas e planejamentos de tarefa

É possível editar as opções de tarefa e o planejamento para alguns tipos de tarefa.

Sobre Esta Tarefa

Para tarefas de restauração, é possível editar as opções de tarefa usando o assistente **Restaurar**.



Para os tipos de tarefa a seguir, é possível editar o planejamento de tarefa:

- Restaurar (tarefas recorrentes)
- Inventário
- Relatar
- Manutenção

Procedimento

Para editar uma tarefa ou um planejamento de tarefa, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.
2. Clique no ícone editar ou planejar.

Opção	Descrição
	Clique neste ícone de edição para abrir o assistente Restaurar e alterar as opções para a tarefa. Siga as instruções para usar o assistente no tópico de restauração de recurso aplicável em Capítulo 10, “Protegendo sistemas virtualizados”, na página 249 e Capítulo 14, “Protegendo bancos de dados”, na página 363.
	Clique neste ícone de edição para alterar o planejamento da tarefa.

Cancelando Tarefas

É possível cancelar uma tarefa que está em execução.

Procedimento

Para cancelar uma tarefa, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Tarefas e Operações** e, em seguida, clique em **Executar Tarefas**.
2. Clique no menu **Ações** que está associado à tarefa e, em seguida, clique em **Cancelar**.

Excluindo Tarefas


É possível excluir uma tarefa de restauração ou de relatório que tenha um status de IDLE.

Sobre Esta Tarefa

Este procedimento se aplica apenas a tarefas de restauração e de relatório. Para excluir uma tarefa de backup, deve-se excluir a política de acordo de nível de serviço (SLA) que está associada a essa tarefa.

Procedimento

Para excluir uma tarefa de restauração ou relatório, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Tarefas e operações** e, em seguida, clique na guia **Planejamento**.
2. Clique no ícone excluir  que está associado à tarefa.

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.

Dica: 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 de tarefa e, em seguida, clique em **Executar Novamente**.
Se a tarefa de backup não puder ser executada novamente, a opção **Executar novamente** não estará disponível.

Resultados

Todas as opções de SLA e quaisquer exclusões que estão associadas à tarefa original são incluídas na operação de nova execução. Todas as mudanças de opção ou exclusão que você aplicou após a última operação de backup parcial são ignoradas. Se a tarefa de nova execução for concluída com sucesso, o resumo da tarefa será atualizado para mostrar sucesso.

Executando uma tarefa de backup ad hoc

Com uma tarefa de backup ad hoc, é possível selecionar um ou mais recursos que estão associados a uma política de SLA e executar uma operação de backup on demand para esses recursos.

Sobre Esta Tarefa


Este recurso associa a política de SLA e os recursos selecionados em uma tarefa ad hoc com o propósito de executar uma operação de backup on demand imediata. Ele não altera as designações de política de SLA para recursos que estão associados às tarefas planejadas.


Procedimento

Para executar uma tarefa de backup ad hoc, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Tarefas e Operações > Criar Tarefa**.
2. Selecione **Backup Ad hoc** para abrir o assistente de backup.

Dicas:

- Você também pode abrir o assistente a partir do hypervisor individual ou de páginas de gerenciamento de aplicativo clicando em **Gerenciar Proteção > Hypervisors** ou **Gerenciar Proteção > Aplicativos**.
 - Para um resumo da execução de suas seleções no assistente, clique em **Visualizar Backup** na área de janela de navegação no assistente.
3. Na página **Tipo de origem**, clique no hypervisor ou aplicativo para obter os recursos que você deseja incluir na tarefa.
 4. Na página **Selecionar Política de SLA**, selecione a política de SLA e, em seguida, clique em **Avançar**.
 5. Na página **Selecionar origem**, tome as ações a seguir:
 - a) Revise os recursos disponíveis.
É possível inserir todo ou parte de um nome na caixa de filtro para localizar recursos que correspondam 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 recurso que você deseja incluir na tarefa.

Para remover um recurso da lista, clique no ícone de menos  ao lado do recurso.
 - c) Clique em **Avançar**.
 6. Na página **Revisar**, revise as configurações da tarefa e, em seguida, clique em **Enviar** para criar e executar a tarefa.

O que Fazer Depois

Para visualizar o status e outras informações sobre a tarefa, clique em **Tarefas e Operações** na área de janela de navegação e clique na tarefa na guia **Tarefas em Execução**.

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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 login 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 login 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 em Linux e scripts de lote e do PowerShell para máquinas baseadas em 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 **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 em 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 504 .

Incluindo um script em um servidor

É possível incluir um script no servidor a partir do qual o script será executado.

Procedimento

Conclua as etapas a seguir para incluir um script em 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 17. 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. Clique na guia **Relatórios**.
3. Selecione **Utilização de Armazenamento de Backup** no menu suspenso **Filtrar por categoria**.
4. Execute o relatório clicando no ícone **Executar Relatório** (🔍) ao lado do relatório desejado.

Os seguintes relatórios estão disponíveis:

Relatório Utilização de Backup da VM

As máquinas virtuais podem ser limitadas pelo uso das caixas de seleção **Tipo de Hypervisor**, **Hypervisor** e **Tags de VM**. O valor padrão é **Todos**, que mostra dados para todos os backups de VM.

O relatório Utilização de Backup da VM inclui o nome da VM, sua localização, o tipo de hypervisor, a política de SLA que é usada para proteger a VM e o local do armazenamento de backup utilizado. Esse retroarmazenamento pode ser o nome do host ou endereço IP de um disco, o nome do servidor em nuvem ou o nome do servidor do repositório. O tamanho do backup de cada VM e o número de pontos de recuperação que estão disponíveis para cada VM que é exibida. Por fim, o número total de máquinas virtuais protegidas aparece na parte inferior do relatório. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório Utilização de Armazenamento do vSnap

Use as opções de relatório para filtrar servidores vSnap específicos para exibição por meio da caixa de seleção **Armazenamento do vSnap**. Para filtrar os volumes de destino de réplica, selecione **Excluir Volumes de Destino de Réplica**. 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**. Essa área do relatório exibe os nomes das máquinas virtuais, o hypervisor associado, local e a proporção de compactação e deduplicação do servidor vSnap.

O relatório Utilização de Armazenamento do vSnap exibe os servidores vSnap, o site, o status, o espaço total, o espaço livre e o espaço utilizado. Quando expandido, as taxas de deduplicação e de compactação, se aplicável, são exibidas para cada servidor vSnap. 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. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Nota: 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 514](#)

É possível executar, salvar ou planejar relatórios no IBM Spectrum Protect Plus.

[“Tipos de relatório” na página 507](#)

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. Clique na guia **Relatórios**.
3. Selecione **Proteção** no menu suspenso **Filtrar por categoria**.
4. Execute o relatório clicando no ícone **Executar Relatório** (🔍) ao lado do relatório desejado.

Os seguintes relatórios estão disponíveis:

Relatório Histórico de Backup do Volume Persistente do Contêiner

O Relatório Histórico de Backup do Volume Persistente do Contêiner exibe o histórico de tarefas anteriores do volume de contêiner persistente. Use as opções de relatório para filtrar por tipo de PVC (Solicitação de Volume Persistente) e para selecionar **PVCs** específicas para exibição. O relatório pode ser ainda mais filtrado por tarefas com falha ou com êxito no campo **Status** e por políticas específicas de acordo de nível de serviço (SLA) usando o campo **Política de SLA**. Configure um valor de número inteiro no campo **Histórico de Backup para os Últimos Dias** para mostrar o histórico de backup por um número especificado de dias.

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 **Status** por tarefas com falha ou bem-sucedidas. O relatório pode ser filtrado ainda mais por políticas específicas de acordo de nível de serviço (SLA) usando o campo **Política de SLA**. Um valor de número inteiro pode ser especificado para o campo **Histórico de backup para número de dias passados** para limitar resultados.

Na visualização de detalhes do relatório, expanda uma tarefa associada para visualizar mais detalhes da tarefa, como a razão pela qual uma tarefa falhou ou o tamanho de um backup bem-sucedido. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório de Conformidade do RPO de Política do SLA

Use as opções de relatório para filtrar por **Tipo de Aplicativo** e para selecionar um **Servidor de Aplicativos** específico para exibição. O relatório pode ser mais filtrado por bancos de dados que estão

em conformidade ou fora de conformidade com o RPO definido por meio do campo **Exibir Bancos de Dados que Estão** ou por **Tipo de Proteção**, incluindo dados que foram submetidos a backup para o vSnap, usando replicação, usando cópia de armazenamento de objeto ou usando archive.

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. A visualização rápida exibe um gráfico de pizza de uma contagem de backups para o vSnap que estão em conformidade e aqueles que não estão em conformidade. A visualização de resumo exibe a política de SLA, o planejamento de SLA, o número de backups para o vSnap que estão em conformidade, o número dos que não estão em conformidade e as replicações que estão em conformidade e fora de conformidade. Também são exibidos bancos de dados que não estão em conformidade para os tipos de proteção, o que inclui os nomes de banco de dados, servidores de aplicativos, tipos de aplicativos, o último tempo de proteção bem-sucedido e o motivo da falta de conformidade.

Relatório Histórico de Backup do Sistema de Arquivos

Execute o relatório Histórico de Backup do Sistema de Arquivos para revisar o histórico de proteção de sistemas de arquivos específicos. Para executar o relatório, pelo menos um servidor deve ser especificado na opção **Servidor** e um sistema de arquivos deve ser selecionado para a opção **Sistema de Arquivos**. Use as opções de relatório para filtrar **Status** por tarefas com falha ou bem-sucedidas. O relatório pode ser filtrado ainda mais por políticas específicas de acordo de nível de serviço (SLA) usando o campo **Política de SLA**. A configuração padrão para todas as quatro opções é **All**. Um valor de número inteiro pode ser especificado para o campo **Histórico de backup para número de dias passados** para limitar resultados.

As propriedades do relatório exibem a data de criação e a conta que foi usada para gerar o relatório. Também estão incluídos os filtros de relatório usados quando o relatório foi gerado. Na visualização de detalhes do relatório, o sistema de arquivos é listado com o servidor e o número total de execuções. A política de SLA, o horário da tarefa e esse status da tarefa são exibidos. As informações podem ser expandidas de uma tarefa associada para visualizar mais detalhes da tarefa, como a razão pela qual uma tarefa falhou e o tamanho de um backup bem-sucedido. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório Conformidade do RPO da Política de SLA do Sistema de Arquivos

Use as opções de relatório para selecionar um **Servidor** específico para exibição. O relatório pode ser mais filtrado pelo **Tipo de Proteção**, incluindo dados que foram submetidos a backup para o vSnap, usando a replicação, usando cópia de armazenamento de objeto ou usando archive. A configuração padrão para esses dois filtros é **All**. Os sistemas de arquivos que estão em conformidade ou fora de conformidade com o RPO definido podem ser filtrados por meio do campo **Exibir Sistemas de Arquivos que Estão**.

O relatório Conformidade do RPO da Política de SLA do Sistema de Arquivos exibe os sistemas de arquivos em relação aos objetivos do ponto de recuperação, conforme definido nas políticas de SLA. As propriedades do relatório exibem a data de criação e a conta que foi usada para gerar o relatório. Também estão incluídos os filtros de relatório usados quando o relatório foi gerado. A visualização rápida exibe um gráfico de pizza de uma contagem de backups para o vSnap que estão em conformidade e aqueles que não estão em conformidade. A visualização de resumo exibe a política de SLA, o planejamento de SLA, o número de backups para vSnap e tarefas usando a replicação. As tarefas de política de SLA do sistema de arquivos fora de conformidade serão incluídas se o filtro de conformidade não estiver selecionado. As informações exibidas são tarefas de SLA fora de conformidade utilizando: backup para vSnap, replicação, cópia de armazenamento de objetos e archive. Para tarefas de política de SLA de sistema de arquivos fora de conformidade, a política de SLA e o planejamento de SLA são listados com cada sistema de arquivos, servidor, o último horário de proteção bem-sucedido e o motivo da falta de conformidade.

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 do servidor de aplicativos, incluindo o número de bancos de dados desprotegidos e protegidos, bem como a capacidade 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 é exibida para cada tipo de banco de dados e fornece mais informações, incluindo nomes de banco de dados, servidor de aplicativos e hospedagem de VM. A visualização de detalhes também fornece essas informações sobre bancos de dados desprotegidos na visualização de detalhes - seção de bancos de dados desprotegidos. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório Sistemas de Arquivos Protegidos e Desprotegidos

Execute o relatório Sistemas de Arquivos Protegidos e Desprotegidos para visualizar o status de proteção de seus sistemas de arquivos. O relatório exibe os sistemas de arquivos protegidos e desprotegidos incluídos no inventário IBM Spectrum Protect Plus antes do início das tarefas de backup. Use as opções de relatório para filtrar por **Servidor**, **Tipo de Sistema Operacional** e **Tipo de Sistema de Arquivos** para exibição. Para excluir sistemas de arquivos que são protegidos através de tarefas de backup baseadas em hypervisor, selecione **Ocultar Sistemas de Arquivos protegidos como parte do Hypervisor Backup**. Para excluir sistemas de arquivos desprotegidos no relatório, selecione **Ocultar Sistemas de Arquivos Desprotegidos**.

As propriedades do relatório exibem a data de criação e a conta que foi usada para gerar o relatório. Também estão incluídos os filtros de relatório usados quando o relatório foi gerado. A visualização de resumo exibe o status de proteção dos sistemas de arquivos registrados. Duas visualizações detalhadas são exibidas, uma para sistemas de arquivos protegidos e a outra para sistemas de arquivos desprotegidos. As informações são organizadas por Sistema de Arquivos, Caminho, Tipo de Sistema de Arquivos, Tipo de SO e Servidor com o número total de sistemas de arquivos protegidos e desprotegidos exibidos. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório VMs Protegidas e Desprotegidas

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 o **Hypervisor/Contas** 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 de Cópia de Armazenamento de Objeto**. **Tags** também podem ser usadas para filtrar relatórios.

As VMs protegidas exibem uma visão geral de suas máquinas virtuais protegidas, incluindo o número total de VMs protegidas, o nome da VM, o hypervisor/conta, tipo de hypervisor, local e a capacidade gerenciada. A capacidade gerenciada é a capacidade utilizada de uma máquina virtual. As VMs desprotegidas fornecem as mesmas informações para máquinas virtuais que não são protegidas. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

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 **Status** por tarefas com falha ou bem-sucedidas. O relatório pode ser filtrado ainda mais por políticas específicas de acordo de nível de serviço (SLA) usando o campo **Política de SLA**. Um número inteiro pode ser especificado para o campo **Histórico de Backup para os Últimos Dias** para limitar resultados. **Tags** também podem ser usadas para filtrar o relatório.

A visualização de detalhes exibe a política de SLA usada listada sob a VM, conta e número total de execuções. As informações para cada execução podem ser expandidas para listar o tamanho dos dados de backup. O tempo de proteção, o status e o armazenamento de backup usado também são exibidos. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório de Conformidade do RPO de Política do VM S

Use as opções de relatório para filtrar por **Tipo, Hypervisor/Conta, Tipo de Proteção**, que inclui dados que foram submetidos a backup para vSnap, usando replicação, usando cópia de armazenamento de objetos, usando archive ou usando captura instantânea e para exibir máquinas virtuais que estão em conformidade ou fora de conformidade com o RPO definido por meio do campo **Exibir VMs que Estão**. Há também um filtro para **Tags**.

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. A visualização rápida exibe um gráfico de pizza de uma contagem de backups para o vSnap que estão em conformidade e aqueles que não estão em conformidade. Também é um gráfico de pizza de capturas instantâneas que estão em conformidade e que não estão em conformidade. Uma visualização de resumo exibe a política de SLA usada, o planejamento de SLA, a proporção de backups para o vSnap em conformidade e fora de conformidade e a proporção de capturas instantâneas em conformidade e fora de conformidade. Também são exibidas VMs fora de conformidade para cada tipo de proteção. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Conceitos relacionados

“Tipos de relatório” na página 507

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. Clique na guia **Relatórios**.
3. Selecione **Sistema** no menu suspenso **Filtrar por categoria**.
4. Execute o relatório clicando no ícone **Executar Relatório** (🔍) ao lado do relatório desejado.

Os seguintes relatórios estão disponíveis:

Relatório de configuração

Use a opção **Tipo de Configuração** para filtrar os tipos de configuração a serem exibidos. O relatório Configuração exibe a configuração dos servidores de aplicativos, sistemas virtualizados, armazenamento de backup para servidores de disco, armazenamento de objeto e servidores de repositório, proxies VADP, servidores LDAP e servidores SMTP. Estão incluídos no relatório o nome do recurso, tipo de recurso (OS ou aplicativo), provedor, site associado, estado e o status de conexão SSL. Nem todas as opções são exibidas para cada componente no relatório Configuração. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório de Tarefa

Use as opções de relatório para filtrar os tipos de tarefas marcando a caixa de seleção **Tipo de Tarefa** e para exibir tarefas que foram executadas com sucesso durante um período de tempo na caixa de seleção **Dias Desde a Execução com Sucesso**. A visualização rápida exibe um gráfico de pizza com o número de tarefas concluídas, tarefas com falha e outras tarefas. A visualização de resumo para tarefas que foram executadas pelo menos uma vez exibe o tipo de tarefa, o número de tarefas associadas a esse tipo, o número de execuções, o número de tarefas concluídas, as tarefas com falha e outras. A visualização de detalhes para tarefas executadas pelo menos uma vez inclui a tarefa, o tipo, o número de execuções e o número de tarefas concluídas, as tarefas com falha e outras tarefas, a última execução bem-sucedida e a porcentagem de sucesso. Em todos os casos, outras tarefas são tarefas que são interrompidas, parcialmente executadas, estão em execução atualmente, ignoradas ou paradas. Na visualização de detalhes, clique no ícone de mais (+) ao lado de uma tarefa associada para visualizar mais detalhes da tarefa, como o ID da tarefa, o tempo médio de execução, o

último status de tempo de execução, último tempo de execução e o próximo tempo de execução planejado, se a tarefa é planejada e os recursos protegidos. No final do relatório está uma visualização de detalhes para tarefas que nunca foram executadas.

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.

Proteção do Office 365

O campo **Proteção do Office 365** exibe os usuários protegidos por meio da tarefa de backup do aplicativo Office 365. O campo **Capacidade Front End** exibe o tamanho total usado dos usuários protegidos.

Proteção de Volume Persistente de Contêiner

O campo **Proteção de Volume Persistente de Contêiner** exibe os volumes persistentes de contêiner protegido. O campo **Capacidade Front End** exibe o tamanho usado desses volumes persistentes de container protegido.

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 507](#)

É possível customizar relatórios predefinidos para monitorar a utilização do armazenamento de backup e outros aspectos do ambiente do sistema.

Executando um relatório de ambiente da VM

É possível executar relatórios para o ambiente da sua Máquina Virtual (VM) em IBM Spectrum Protect Plus. Os relatórios podem ajudá-lo a monitorar a quantidade de espaço livre em cada hypervisor, o uso de armazenamento de números de unidades lógicas (LUNs) e o status de todas as VMs.

Procedimento

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Clique na guia **Relatórios**.
3. Selecione **Ambiente de VM** no menu suspenso **Filtrar por Categoria**.
4. Execute o relatório clicando no ícone **Executar Relatório** (▶) ao lado do relatório desejado.

Os seguintes relatórios estão disponíveis:

Relatório Armazenamento de Dados da VM

Escolha para revisar a utilização de armazenamento dos armazenamentos de dados em seu ambiente de VM. As informações que esse relatório fornece podem ser filtradas usando o **Tipo de Hypervisor** e o **Hypervisor**. O **Filtro de Visualização de Detalhes** controla os armazenamentos de dados a serem exibidos na visualização de detalhes com base na porcentagem de espaço

utilizada. 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.

A visualização rápida exibe um gráfico de pizza com a utilização de armazenamento de espaço livre e usado. A visualização de resumo exibe o hypervisor, a contagem de armazenamentos de dados, a capacidade e o espaço livre. A visualização de detalhes mostra os armazenamentos de dados e exibe armazenamentos de dados órfãos que não possuem VMs registradas. Também é exibido o hypervisor associado, o tipo de hypervisor, o tipo de armazenamento de dados, a capacidade, o espaço livre e a porcentagem utilizada. Todas as três visualizações contêm o total de armazenamentos de dados, a capacidade total e o espaço livre total. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório de VM LUNs

Revise a utilização de armazenamento de seus números da unidade lógica (LUNs) da máquina virtual. Os filtros para esse tipo de relatório incluem **Tipo de Hypervisor** e **Hypervisors**. 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.

No relatório, a visualização do resumo exibe o hypervisor, o número de LUNs associados ao hypervisor e a capacidade. Na visualização de detalhes, é exibido o nome do LUN, o ID do LUN, o fornecedor de armazenamento, o hypervisor, o armazenamento de dados ou volume, a capacidade, o tipo de transporte e o mapeamento de dispositivo bruto para cada LUN. Ambas as visualizações exibem a contagem total de LUN e a capacidade total. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Relatório da VM Snapshot Sprawl

Este relatório de expansão de captura instantânea exibe a idade, o nome e o número de capturas instantâneas que são usados para proteger seus recursos do Hypervisor. As opções de relatório disponíveis pelas quais filtrar são **Tipo de Hypervisor**, **Hypervisor** e **Tags**. Use o filtro **Horário de criação de captura instantânea** para exibir capturas instantâneas de períodos de tempo específicos.

O relatório contém uma visualização de detalhes que exibe o nome da captura instantânea e o horário de criação da captura instantânea. Cada captura instantânea aparece sob o tipo de VM, hypervisor e hypervisor associado. O número total de VMs e capturas instantâneas é exibido no final da visualização. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

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. As opções de relatório disponíveis pelas quais filtrar são **Tipo de Hypervisor**, **Hypervisor**, **Dias Desde o Último Desligamento**, **Dias Desde a Última Suspensão**, **Dias Desde o Último Ligamento** e **Tags**.

O relatório contém a visualização rápida que é um gráfico de pizza que exibe a utilização de armazenamento com base no estado da energia da máquina virtual: VMs desligadas, VMs ligadas, modelos e VMs suspensas. Há também visualizações de detalhes para cada um dos estados de energia. A visualização de detalhes - VMs desligadas exibe o nome da VM, a data e o número de dias desde o desligamento, o hypervisor associado, o tipo de hypervisor, o espaço fornecido e o armazenamento de dados ou volume. O total de VMs desligadas é exibido na parte inferior dessa visualização, juntamente com o espaço total fornecido. A visualização de detalhes - VMs suspensas contêm o nome da VM, a data e o número de dias desde que a VM foi suspensa, o hypervisor associado, o tipo de hypervisor, o espaço fornecido e o armazenamento de dados ou volume. O número total de VMs suspensas e o espaço total fornecido são exibido na parte inferior da visualização. A visualização de detalhes - modelos contém os nomes de modelo, o hypervisor associado, o tipo de hypervisor, o espaço fornecido e o armazenamento de dados ou volume. O

total de modelo e o espaço total fornecido aparecem na parte inferior da visualização. A visualização de detalhes - VMs ligadas contém o nome da VM, a data e o número de dias que a VM ficou ligada, o hypervisor associado, o tipo de hypervisor, o espaço fornecido e o armazenamento de dados ou volume. No final da visualização está o número total de VMs ligadas e o espaço total fornecido. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

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 pelas quais filtrar o **Tipo de Hypervisor** e para selecionar qual **Hypervisor** exibir.

O relatório contém uma visualização de detalhes que exibe o nome da VM e o espaço fornecido. Cada VM aparece sob o tipo de armazenamento de dados ou volume, hypervisor e tipo de hypervisor. O número total de armazenamentos de dados/volumes e VMs é exibido no final da visualização. A caixa **Procurar** pode ser usada para filtrar ainda mais os resultados do relatório.

Conceitos relacionados

[“Tipos de relatório” na página 507](#)

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.

Antes de Iniciar

As funções customizadas que são designadas aos usuários que executam relatórios requerem que as permissões apropriadas sejam definidas nessa função para que o relatório possa ser visualizado. Para obter mais informações sobre funções, tipos de permissão e permissões, consulte [“Gerenciando atribuições” na página 521](#).

Procedimento

Para executar um relatório, conclua as seguintes etapas:

1. Na área de janela de navegação, clique em **Relatórios e logs > Relatórios**.
2. Clique na guia **Relatórios**.
3. Execute o relatório clicando no ícone **Executar Relatório** () ao lado do relatório desejado.
 - Para executar o relatório com parâmetros customizados, configure os parâmetros na janela **Executar relatório** 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 507](#)

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. Clique na guia **Relatórios**.
3. Clique no ícone **Criar Relatório Customizado** (+) ao lado do relatório desejado para ser customizado.
4. Na janela **Criar Relatório Customizado**, selecione a guia **Parâmetros**. Digite um nome para o relatório no campo **Nome** e digite uma descrição para o relatório customizado no campo **Descrição**. Configure seus parâmetros customizados que se relacionam com o relatório selecionado.

Nota: Os nomes de relatórios podem incluir caracteres alfanuméricos e os símbolos a seguir: \$-_.+!*'(). Os espaços não são permitidos no nome do relatório.

5. Opcionalmente, na guia **Planejamento**, marque a caixa **Definir Planejamento**. Se um planejamento tiver que ser definido, forneça estas informações:

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

- Para **Frequência**, insira um valor de número inteiro e selecione **Minutos**, **Horas**, **Dias**, **Semanas**, **Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.
- Para **Horário de início**, insira uma data e hora e selecione o fuso horário apropriado. O fuso horário padrão que é exibido é baseado nas configurações do navegador
- Insira o endereço de e-mail do destinatário que deve receber uma cópia do relatório no campo de endereço de e-mail. Pelo menos um destinatário deve ser incluído. Se forem necessários mais endereços, clique no ícone de mais **Incluir um Destinatário** (+).

6. Clique no botão **Salvar Relatório**.
7. Para localizar um relatório customizado, clique na guia **Relatórios Customizados**.
8. Clique no ícone **Executar Relatório Customizado** (play) para executar o relatório.
9. Opcionalmente, para atualizar um relatório customizado, clique no ícone **Atualizar Relatório Customizado** (pencil). Para remover um relatório customizado, clique no ícone **Remover Relatório** (X).

O que Fazer Depois

Execute o relatório customizado e revise os resultados do relatório.

Conceitos relacionados

[“Gerenciando relatórios e logs” na página 507](#)

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 em IBM Spectrum Protect Plus para serem executados 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. Clique na guia **Relatórios**.
3. Defina um planejamento para um relatório clicando no ícone **Planejar relatório com parâmetros padrão** () ao lado do relatório desejado.

Nota: Para planejar um relatório com parâmetros não padrão, crie um relatório customizado. Para obter mais informações, consulte [“Criando um Relatório Customizado”](#) na página 515.

4. Aparecerá a janela **Planejar relatório com parâmetros padrão**.

Restrição: Os dias da semana para a opção **Semanas** estarão disponíveis somente se você instalar a correção temporária 10.1.6 eFix2 ou posterior do IBM Spectrum Protect Plus.

- Para **Frequência**, insira um valor de número inteiro e selecione **Minutos, Horas, Dias, Semanas, Meses** ou **Anos**. Quando a opção **Semanas** é selecionada, é possível escolher um ou mais dias da semana. O **Horário de Início** se aplicará aos dias da semana selecionados.
- Para **Horário de início**, insira uma data e hora e selecione o fuso horário apropriado. O fuso horário padrão que é exibido é baseado em suas configurações do navegador da web.
- Insira o endereço de e-mail do destinatário que deve receber uma cópia do relatório no campo de endereço de e-mail. Pelo menos um destinatário deve ser incluído. Se forem necessários mais endereços, clique no ícone de mais **Incluir um Destinatário** ()

5. Clique no botão **Planejar**.

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 507


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 526

Antes de um usuário poder efetuar login no IBM Spectrum Protect Plus e usar as funções disponíveis, uma conta do usuário deve ser criada no IBM Spectrum Protect Plus.

Capítulo 18. 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.

Restrição: Não designe um usuário de controle de acesso baseado em função (RBAC) a mais de um grupo de recursos VMware. Os usuários que foram designados ao grupo de recursos Tag e Categorias e depois também são designados a Hosts e Clusters ou VMs e Modelos farão com que os dados não sejam exibidos para a visualização Hosts e Clusters ou visualização VMs e Modelos. Somente as informações para Tags e Categorias serão exibidas quando forem selecionadas como uma visualização durante a execução de operações.

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 a SQL e o Exchange ocupam a mesma máquina e ambos são registrados com o IBM Spectrum Protect Plus, apenas um desses poderá ser incluído como um servidor de aplicativos para 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 519.</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 523.

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.
Contêiner	Kubernetes	Usado para conceder acesso a recursos de contêiner.
Sistema de Arquivos	Windows	Usado para conceder acesso a recursos do sistema de arquivos.
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• Amazon EC2	Usado para conceder acesso a recursos do sistema virtualizado.
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.

Tipo de Recurso	Subtipo	Descrição
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.
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 a SQL e o Exchange ocupam a mesma máquina e ambos são registrados com o IBM Spectrum Protect Plus, apenas um desses poderá ser incluído como um servidor de aplicativos para 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.

Da mesma forma, as permissões podem ser configuradas para criar contas de administrador, permitindo que um usuário crie e edite outras contas, configure sites e recursos e interaja com todos os recursos do IBM Spectrum Protect Plus disponíveis.

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

Os usuários com o Admin do Aplicativo podem concluir as ações a seguir:

- Registrar e modificar recursos do banco de dados do aplicativo que são delegados por um administrador
- Associar bancos de dados de aplicativos a políticas de SLA designadas
- Operações de backup e de restauração completas
- Executar e planejar 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

Os usuários com a função Apenas Backup podem concluir as ações a seguir:

- Criar, visualizar e executar 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**.

OC_MONITOR_ROLE

O OC_MONITOR_ROLE é criado quando um usuário OC_MONITOR é criado pelo IBM Spectrum Protect Operations Center. Essa função e o usuário são requeridos pelo Operations Center para conectar-se ao ambiente do IBM Spectrum Protect Plus. O OC_MONITOR_ROLE é usado apenas pelo usuário OC_MONITOR e fornece permissões que são necessárias para conectar o Operations Center ao IBM Spectrum Protect Plus. Não edite essa função.

Restaurar Apenas

Os usuários com a função Restaurar Apenas podem concluir as ações a seguir:

- 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

Os usuários com a função Autoatendimento podem monitorar 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 ações a seguir para todos os usuários que não sejam admin com a função SUPERUSER:

- Modificar e excluir contas do usuário
- Alterar senhas do usuário
- Designar funções de usuário

Admin de VM

Os usuários com a função Admin de VM podem concluir as ações a seguir:

- Registrar e modificar recursos do hypervisor aos quais o usuário tem acesso
- Associar hypervisors a políticas de SLA

- Operações de backup e de restauração completas
- Executar e planejar 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 523.</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.

Nome	Permissões	Descrição
Armazenamento de Objeto	Register, view, edit, deregister	Usado para interagir com armazenamento de objetos que é definido como armazenamento de backup para operações de cópia.
Nuvem	Register, view, edit, deregister	Usado para interagir com servidores em nuvem que são definidos como armazenamento de backup para operações de cópia.
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.
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 Manter , Liberar , Release e Executar ações de restauração customizadas 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.

Nome	Permissões	Descrição
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.
Servidor de Script	Register, view, edit, deregister	Usado para interagir com o servidor no qual prescripts e postscripts são executados.
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.
Usuário	Criar, visualizar, editar, excluir	Usado para interagir com usuários, associar um grupo de recursos a uma função e fornecer 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 login 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 518 e [“Criando uma função”](#) na página 523.

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

Com o IBM Spectrum Protect Plus, é possível usar um servidor Lightweight Directory Access Protocol (LDAP) para gerenciar usuários. Ao criar uma conta do usuário LDAP, é possível incluir a conta do usuário em um grupo de usuários.

Antes de Iniciar

Execute as seguintes tarefas:

- Assegure-se de ter registrado um provedor LDAP com IBM Spectrum Protect Plus. Para registrar um provedor LDAP, siga as instruções em [“Incluindo um servidor LDAP”](#) na página 207.
- Se você deseja usar funções customizadas e grupos de recursos, assegure-se de que as funções ou grupos estejam disponíveis. Para instruções sobre criação de funções e grupos, consulte [“Criando uma função”](#) na página 523 e [“Criando um Grupo de Recursos”](#) na página 518.

Procedimento

Para criar uma conta de usuário para um grupo LDAP, conclua as etapas a seguir:

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. No campo **Nome do Grupo** da seção **Selecionar Grupo LDAP**, especifique o grupo LDAP executando uma das ações a seguir:
 - Insira o nome do grupo LDAP.
 - Procure o nome do grupo LDAP inserindo um texto parcial, um asterisco (*) como um caractere curinga único ou um ponto de interrogação (?) para correspondência de padrões. Para visualizar todos os grupos LDAP, clique no botão **Visualizar Todos**.
 - Opcionalmente, um nome distinto relativo (RDN) pode ser fornecido preenchendo o campo **Grupo RDN**.
5. Os Grupos LDAP são exibidos na tabela **Grupos LDAP**. Selecione um Grupo LDAP.
6. Na seção **Designar função**, selecione uma ou mais funções para o usuário.
7. Na seção **Grupos de permissão**, revise as permissões e recursos que estão disponíveis para o usuário e, em seguida, clique em **Continuar**.
8. 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**.
9. Clique em **Criar usuário**.

Resultados

A conta do usuário é exibida na tabela de usuários. Opcionalmente, para visualizar funções, permissões e grupos de recursos disponíveis, selecione um usuário na tabela de usuários.

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.

Password

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 19. 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 IBM Spectrum Protect Plus a partir de uma liberação prévia, deve-se executar a tarefa de manutenção para atualizar os 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 495](#)

As tarefas são usadas para executar operações de backup, restauração, manutenção, inventário e relatório em IBM Spectrum Protect Plus.

Tarefas relacionadas

[“Iniciando tarefas sob demanda” na página 497](#)

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 20. 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 567387](#).

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.

Como criar camadas de dados para o armazenamento em fita ou em nuvem?

Não é possível criar camadas de dados do IBM Spectrum Protect Plus para o armazenamento em fita. É possível criar camadas de dados do IBM Spectrum Protect Plus para armazenamento em nuvem, mas apenas para classes de armazenamento em nuvem que suportam o rápido recall de dados. Quando você estiver copiando dados para fita do IBM Spectrum Protect Plus para o Servidor IBM Spectrum Protect, não será uma boa ideia usar a função hierárquica do IBM Spectrum Protect. Se você estiver arquivando dados para fita, deverá usar um conjunto de armazenamentos em cache frio.

Revise as diretrizes sobre armazenamento em fita e em nuvem:

- Embora você não possa criar camadas de dados do IBM Spectrum Protect Plus para fita, é possível arquivar ou copiar os dados do IBM Spectrum Protect Plus em fita. Para isso, defina um conjunto de armazenamentos de cache de dados frios, conforme descrito na Etapa 1: criando um conjunto de armazenamento em fita e um conjunto de armazenamentos de cache de dados frios para copiar dados na fita.
- É possível criar camadas de dados do IBM Spectrum Protect Plus para conjuntos de armazenamentos de contêineres em nuvem, mas apenas para classes de armazenamento em nuvem que suportam o rápido recall de dados. Se você estiver usando o Amazon Web Services (AWS) com o protocolo do Simple Storage Service (S3) para mover dados para conjuntos de contêineres em nuvem, não mova os dados para a Amazon S3 Glacier. Para obter cenários e instruções sobre como copiar ou arquivar dados para armazenamento em nuvem, consulte Configuração para copiar ou arquivar dados. Para obter instruções sobre a criação de camadas de dados para a nuvem, consulte Criando camadas de dados para armazenamento em nuvem ou fita na documentação do produto IBM Spectrum Protect.

Não é possível criar camadas de dados do IBM Spectrum Protect Plus para fita. Para armazenar os dados do IBM Spectrum Protect Plus em fita, copie os dados para um servidor IBM Spectrum Protect para armazenamento em mídia de fita física ou em uma biblioteca de fitas virtual. Para cenários diferentes e para obter mais informações sobre como configurar o armazenamento, consulte [“Configuração para copiar ou arquivar dados para IBM Spectrum Protect”](#) na página 190 e [“Configuração para copiar ou arquivar dados na nuvem”](#) na página 183. Você

Para configurar um conjunto de armazenamento de cache frio para arquivar ou copiar dados para fita, consulte [“Etapa 1: criando um conjunto de armazenamento em fita e um conjunto de armazenamento em cache de dados frios para copiar dados para fita”](#) na página 193.

Resolução de Problemas do Suporte de Backup de Kubernetes

Para ajudar a solucionar problemas com Suporte de Backup de Kubernetes, é possível coletar arquivos de log de depuração e visualizar logs de rastreo. Também é possível seguir procedimentos para diagnosticar problemas.

Coletando arquivos de log do Suporte de Backup de Kubernetes para resolução de problemas

É possível gerar arquivos de log de depuração no ambiente de Kubernetes para solucionar problemas na implementação de operações Suporte de Backup de Kubernetes e Suporte de Backup de Kubernetes no servidor IBM Spectrum Protect Plus.

Sobre Esta Tarefa

Todos os logs são coletados no diretório /tmp no sistema local e empacotados em um archive tar.gz. Normalmente, o archive é denominado `baas_debug_logs_timestamp.tar.gz`.

Procedimento

Use um dos métodos a seguir para coletar logs para resolução de problemas:

- Para coletar apenas logs do Kubernetes para fins de depuração, emita o comando a seguir:

```
./baas_install.sh -l
```

Esse comando coleta logs de depuração para a implementação do Suporte de Backup de Kubernetes que é especificada pelos parâmetros no `baas_config.cfg`. As informações e logs de estado atuais dos componentes Suporte de Backup de Kubernetes no cluster de Kubernetes são coletados. Os logs são estruturados com base na arquitetura de criação de log básica do Kubernetes. Para obter mais informações, consulte [Criação de log básica em Kubernetes](#).

- Para coletar o pacote de log que inclui os logs de depuração para a implementação do Suporte de Backup de Kubernetes e do servidor IBM Spectrum Protect Plus, emita o comando a seguir:

```
./baas_install.sh -l -x
```

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 assistência.

Tarefas relacionadas

[“Configurando o nível de rastreo de arquivos de log”](#) na página 535

É possível configurar o nível de rastreo de arquivos de log locais para ajudar a solucionar problemas que você pode encontrar no Suporte de Backup de Kubernetes.

Referências relacionadas

“Resolução de problemas de referência rápida” na página 537

Soluções para problemas básicos do Suporte de Backup de Kubernetes são fornecidas.

“Resolução de problemas de operações do Suporte de Backup de Kubernetes” na página 541

Os procedimentos de resolução de problemas estão disponíveis para ajudá-lo a diagnosticar e resolver problemas do Suporte de Backup de Kubernetes.

Configurando o nível de rastreo de arquivos de log

É possível configurar o nível de rastreo de arquivos de log locais para ajudar a solucionar problemas que você pode encontrar no Suporte de Backup de Kubernetes.

Sobre Esta Tarefa

É possível configurar os níveis de rastreo para solucionar problemas com os componentes de gerenciador de transações, controlador e planejador do Suporte de Backup de Kubernetes. O nível de rastreo que você configurou também se aplica aos níveis de log para o agente Suporte de Backup de Kubernetes, assim como os níveis de log nas tarefas de log do IBM Spectrum Protect Plus e arquivo `command.log`.

O componente do movedor de dados não é afetado por essa configuração.

Para configurar o nível de rastreo, deve-se atualizar o arquivo de configuração `baas_config.cfg` e, em seguida, atualizar a implementação do Suporte de Backup de Kubernetes.

Dica: O nível de rastreo padrão é INFO. Se você estiver enfrentando problemas que requerem resolução, configure o nível de rastreo para DEBUG.

Procedimento

Para configurar o nível de rastreo, complete as seguintes etapas na linha de comando de Kubernetes:

1. Efetue login no sistema operacional no nó principal do cluster de Kubernetes que é usado como o nó de instalação.
2. Acesse o diretório em que o pacote de instalação do `SPP_V10.1.6_for_Containers.tar.gz` foi descompactado.
3. Acesse o diretório `installer` emitindo o comando a seguir:

```
cd installer
```

4. Edite o arquivo `baas_config.cfg` com um editor de texto e modifique o valor para o parâmetro **PRODUCT_LOGLEVEL**.

As opções de rastreo a seguir estão disponíveis:

DEBUG

Exibe mensagens de nível de depuração nos arquivos de log do gerenciador de transações, controlador e planejador.

INFO

Exibe todas as mensagens do usuário nos arquivos de log do gerenciador de transações, controlador e planejador, incluindo mensagens de informações, aviso e erro. Esse valor é o padrão.

WARNING

Exibe mensagens de aviso e de erro nos arquivos de log do gerenciador de transações, controlador e planejador.

ERROR

Exibe apenas mensagens de erro nos arquivos de log do gerenciador de transações, controlador e planejador.

Por exemplo, para configurar o nível de rastreo para o modo de depuração, configure o parâmetro **PRODUCT_LOGLEVEL** como a seguir:

```
PRODUCT_LOGLEVEL="DEBUG"
```

- Atualize a implementação do Suporte de Backup de Kubernetes emitindo o comando a seguir:

```
./baas_install.sh -u
```

Quando solicitado, insira *sim* para continuar.

- Opcional: Para verificar o status da atualização, emita o comando a seguir:

```
./baas_install.sh -s
```

Dica: Alternativamente, verifique o status da atualização usando o comando **./helm status baas**.

O que Fazer Depois

É possível coletar arquivos de log do Suporte de Backup de Kubernetes para resolução de problemas ou usar uma ferramenta de visualização, como Kibana, para visualizar e consultar dados nos arquivos de log do gerenciador de transações, controlador e planejador. Para obter instruções, consulte:

- “Coletando arquivos de log do Suporte de Backup de Kubernetes para resolução de problemas” na [página 534](#)
- “Visualizando logs de rastreo para Suporte de Backup de Kubernetes” na [página 536](#)

Visualizando logs de rastreo para Suporte de Backup de Kubernetes

Opcionalmente, é possível utilizar a pilha Elasticsearch, Fluentd, and Kibana (EFK) para visualizar e analisar logs de rastreo que são produzidos por Suporte de Backup de Kubernetes.

Elasticsearch é um mecanismo de procura de texto completa distribuído. Fluentd é uma ferramenta que coleta logs de nós de cluster e envia os logs para o mecanismo Elasticsearch. Kibana é uma ferramenta de visualização para Elasticsearch com uma interface com o usuário da web e ferramenta de desenvolvimento que é usada para consulta de dados.

Antes de Iniciar

Execute as seguintes etapas:

- Implemente a pilha EFK para o seu cluster de Kubernetes:
 - Implemente o mecanismo de procura Elasticsearch. Para obter instruções, consulte [Instalando o Elasticsearch](#).
 - Implemente o coletor de log Fluentd em cada nó do cluster. Para obter instruções, consulte o [Documentação FluentD](#).
 - Implemente a ferramenta de visualização Kibana. Para obter instruções, consulte o [Guia Kibana](#).
- Conclua a implementação da pilha EFK incluindo um índice logstash no Kibana:
 - Acesse a interface com o usuário do Kibana abrindo um navegador da web e inserindo a URL do computador em que o Kibana está em execução e especifique o número da porta. Por exemplo, especifique uma das URLs a seguir em seu navegador da web:

```
https://localhost:5601
```

ou

```
http://your_domain.com:5601
```

em que *your_domain* especifica o nome de domínio para o computador.

- Se forem oferecidas opções para explorar dados, selecione **Explore on my own**.
- Clique em **Discover** > **Create Index Pattern** e crie o padrão de índice logstash-*

Sobre Esta Tarefa

Quando você usa a pilha EFK, os logs de todos os componentes do contêiner são mesclados e mostrados na mesma visualização. Quaisquer logs para pods interrompidos são preservados no armazenamento de dados persistentes Elasticsearch. É possível aplicar filtros para exibir erros ou mensagens específicas. Você também pode aplicar um filtro de tempo para mostrar eventos que ocorreram em um período de tempo específico.

Além das mensagens de erro e depuração, é possível visualizar logs de rastreo para os seguintes componentes do Suporte de Backup de Kubernetes:

- Gerenciador de transações
- Comunicação
- Planejador

Procedimento

Para visualizar logs de transações para Suporte de Backup de Kubernetes, conclua as etapas a seguir:

1. Abra a interface com o usuário do Kibana e clique no ícone **Discover**.
2. Clique no índice `logstash-*`.
3. Para visualizar logs para Suporte de Backup de Kubernetes, inclua um filtro, tomando as seguintes ações:
 - a) Clique em **Incluir filtro** e especifique os seguintes valores de filtro:
 - Campo: `kubernetes.container_image`
 - Operador: `is`
 - Valor: `baas-`
 - b) Insira um nome para a procura e clique em **Salvar**.
Os contêineres de rastreo para os contêineres `baas-transaction-manager`, `baas-controller` e `baas-scheduler` são exibidos.
4. É possível criar filtros adicionais para mostrar visualizações mais granulares de logs de rastreo do Suporte de Backup de Kubernetes.

Tabela 65. Filtros para visualização de logs de rastreo do Suporte de Backup de Kubernetes		
Tipo de dados para mostrar	Filtro 1	Filtro 2
Logs do gerenciador de transações	<code>kubernetes.container_image is baas-transaction-manager</code>	Nenhuma
Logs do controlador	<code>kubernetes.container_image is baas-controller</code>	Nenhuma
Logs do planejador	<code>kubernetes.container_image is baas-scheduler</code>	Nenhuma
Mensagens de erro	<code>kubernetes.container_image is baas-</code>	<code>log is ERROR</code>
Depurando Mensagens	<code>kubernetes.container_image is baas-</code>	<code>log is DEBUG</code>

Resolução de problemas de referência rápida

Soluções para problemas básicos do Suporte de Backup de Kubernetes são fornecidas.

Use as soluções na tabela a seguir para resolver problemas básicos que podem ocorrer com operações Suporte de Backup de Kubernetes. Se você ainda não puder resolver um problema, consulte [“Resolução de problemas de operações do Suporte de Backup de Kubernetes”](#) na página 541 para procedimentos de resolução de problemas mais detalhados.

Tabela 66. Soluções para problemas básicos

Problema	Solução
<p>A solicitação Suporte de Backup de Kubernetes é inválida.</p> <p>Por exemplo, o campo Backupstatus ou Restorestatus é listado como inválido ao executar o comando a seguir:</p> <pre>kubect1 describe baasreq request_name -n namespace</pre> <p>em que:</p> <p>request_name O nome da solicitação de backup ou restauração. Para solicitações de backup, o valor é o nome da solicitação de volume persistente (PVC). Para solicitações de restauração, o nome deve ser exclusivo e não deve ser o mesmo que o nome da PVC.</p> <p>namespace O espaço de nomes no qual a PVC existe.</p>	<p>Certifique-se de que a solicitação esteja estruturada corretamente verificando os elementos a seguir no arquivo YAML:</p> <ul style="list-style-type: none"> • Assegure-se de que nenhum erro tipográfico exista. • Assegure-se de que as maiúsculas e minúsculas corretas sejam usadas nas instruções. Kubernetes faz distinção entre maiúsculas e minúsculas. <p>Por exemplo, assegure-se de que a declaração de versão da API esteja listada como <code>apiVersion</code> e não <code>apiversion</code>.</p> <ul style="list-style-type: none"> • Para solicitações de restauração: <ul style="list-style-type: none"> – Assegure-se de que o registro de data e hora para um ponto de restauração seja especificado corretamente no campo restorepoint. – Assegure-se de que o tipo de restauração esteja especificado corretamente no campo restoretype. <p>Para obter mais informações, consulte “Restaurando dados do contêiner usando a linha de comandos” na página 348.</p>
<p>As capturas instantâneas estão falhando.</p>	<p>Execute uma ou mais das ações a seguir:</p> <ul style="list-style-type: none"> • Verifique a configuração do Ceph-CSI para assegurar que seus contêineres estejam executando corretamente. O software CSI é necessário para backups de captura instantânea. • Assegure-se de que uma classe de captura instantânea de volume esteja definida para os PVCs que estão sendo submetidos a backup. • Assegure-se de que o segredo esteja no espaço de nomes correto (o espaço de nomes para a PVC). • Assegure-se de que as configurações estejam corretas no ConfigMap (baas-configmap). <p>Para obter mais informações, consulte “Resolução de problemas com tarefas de backup de captura instantânea” na página 542.</p>

Tabela 66. Soluções para problemas básicos (continuação)

Problema	Solução
O movedor de dados falha ao iniciar.	<p>Execute uma ou mais das ações a seguir:</p> <ul style="list-style-type: none"> • Assegure-se de que o volume Ceph RBD esteja montado. É possível verificar se o volume Ceph RBD está falhando na montagem emitindo o comando kubect1 describe no pod do movedor de dados. • Na saída do comando kubect1 describe, verifique os eventos para assegurar que o volume tenha sido inicializado executando a PVC como parte de outro pod em modo de leitura / gravação. • Na saída do comando kubect1 describe, verifique se há eventos de falha de autenticação. Para resolver erros de autenticação, assegure-se de estar executando um registro do Docker seguro. Assegure-se de que o segredo de pull esteja no espaço de nomes da PVC. Para obter instruções, consulte Extrair uma Imagem de um Registro Privado.
O acesso é negado ou a conexão falha durante a montagem de volumes NFS do servidor vSnap.	<p>Execute uma ou mais das ações a seguir:</p> <ul style="list-style-type: none"> • Verifique a política de rede do movedor de dados. Assegure-se de que os endereços do servidor vSnap correspondam aos endereços do servidor IBM Spectrum Protect Plus. • Assegure-se de que uma conexão direta do cluster de Kubernetes com o servidor vSnap IBM Spectrum Protect Plus exista. A conexão por proxies não é suportada.
O planejador, o gerenciador de transações e os pods do controlador foram iniciados, mas cada pod continua reiniciando. Na saída do comando kubect1 describe para o pod do gerenciador de transações, os eventos indicam que a análise de atividade falhou.	<p>Verifique se os valores para os parâmetros CLUSTER_API_SERVER_IP_ADDRESS e CLUSTER_API_SERVER_PORT estão especificados corretamente no arquivo de configuração baas_config.cfg.</p> <p>Se você atualizar os valores no arquivo baas_config.cfg, emita o comando a seguir para atualizar a configuração:</p> <pre>./baas_install.sh -u</pre> <p>Como alternativa, é possível desinstalar e reinstalar Suporte de Backup de Kubernetes para limpar os arquivos de log anteriores. Para obter instruções, consulte “Desinstalando o Suporte de Backup de Kubernetes” na página 157 e “Instalando e implementando imagens do Suporte de Backup de Kubernetes no ambiente de Kubernetes” na página 152.</p>

Tabela 66. Soluções para problemas básicos (continuação)

Problema	Solução
Um objeto Kubernetes persiste no estado de finalização.	<p>Emita o seguinte comando:</p> <pre>kubectl delete object object_name --force --grace-period=0</pre> <p>Se o objeto continuar em estado de finalização, emita o seguinte comando:</p> <pre>kubectl patch object -n namespace object_name -p '{"metadata":{"finalizers":null}}'</pre> <p>Em que:</p> <ul style="list-style-type: none"> • <i>object</i> é um tipo de objeto em Kubernetes, como uma implementação, pod, volume persistente (PV) ou PVC • <i>object_name</i> é o nome do objeto • <i>namespace</i> é o nome do namespace em que o objeto está
O Suporte de Backup de Kubernetes não foi perfeitamente desinstalado.	<p>Limpe manualmente o seu ambiente emitindo os comandos a seguir:</p> <pre>kubectl delete namespace baas kubectl delete clusterrole baas-controller kubectl delete clusterrole baas-scheduler kubectl delete clusterrole baas-spp-agent kubectl delete clusterrole baas-transaction-manager kubectl delete clusterrole aggregate-basreqs-admin-edit kubectl delete clusterrolebinding baas-controller kubectl delete clusterrolebinding baas-scheduler kubectl delete clusterrolebinding baas-spp-agent kubectl delete clusterrolebinding baas-transaction-manager kubectl delete customresourcedefinition baasreqs.baas.io</pre>

Tabela 66. Soluções para problemas básicos (continuação)

Problema	Solução
O cancelamento de uma tarefa de backup de cópia faz com que alguns recursos sejam deixados para trás.	<p>Limpe os recursos restantes concluindo as etapas a seguir:</p> <ol style="list-style-type: none"> 1. Exclua a implementação do movedor de dados emitindo os comandos a seguir: <pre>kubectl get deploy -n namespace kubectl delete deploy --all -n namespace</pre> 2. Exclua a conta de serviço emitindo os comandos a seguir: <pre>kubectl get serviceaccount -n namespace kubectl delete serviceaccount --all -n namespace</pre> 3. Exclua a política de rede emitindo os comandos a seguir: <pre>kubectl get networkpolicy -n namespace kubectl delete networkpolicy --all -n namespace</pre> 4. Exclua o PVC e PV: <p>Um PVC que é criado durante uma operação de backup de cópia tem a seguinte convenção de nomenclatura:</p> <pre>pvc-backup-pvcname-jobid-job_timestamp</pre> <p>Emita os comandos a seguir:</p> <pre>kubectl get pvc -n namespace grep pvc-backup kubectl get pvc -n namespace grep pvc-backup awk '{print \$1}' xargs kubectl delete pvc -n namespace</pre> <p>Se alguma PV permanecer, emita os comandos a seguir:</p> <pre>kubectl get pv grep pvc-backup kubectl get pv grep pvc-backup awk '{print \$1}' xargs kubectl delete pv</pre> 5. Se necessário, remova os objetos volumesnapshot e volumesnapshotcontent, emitindo os comandos a seguir: <pre>kubectl get volumesnapshot -n namespace kubectl get volumesnapshotcontent</pre>

Tarefas relacionadas

“Coletando arquivos de log do Suporte de Backup de Kubernetes para resolução de problemas” na página 534

É possível gerar arquivos de log de depuração no ambiente de Kubernetes para solucionar problemas na implementação de operações Suporte de Backup de Kubernetes e Suporte de Backup de Kubernetes no servidor IBM Spectrum Protect Plus .

Resolução de problemas de operações do Suporte de Backup de Kubernetes

Os procedimentos de resolução de problemas estão disponíveis para ajudá-lo a diagnosticar e resolver problemas do Suporte de Backup de Kubernetes.

As instruções a seguir são fornecidas:

- “Visualizando Arquivos de Log” na página 542
- “Resolução de problemas com tarefas de backup de captura instantânea” na página 542

- [“Resolução de problemas com tarefas de backup de cópia” na página 543](#)
- [“Resolução de problemas de tarefas de restauração” na página 545](#)

Visualizando Arquivos de Log

Para solucionar problemas do Suporte de Backup de Kubernetes, comece visualizando informações nos arquivos de log. Os arquivos de log estão disponíveis para os componentes do gerenciador de transações, controlador e planejador do Suporte de Backup de Kubernetes.

É possível visualizar os arquivos de log para vários componentes do gerenciador de transações. Por exemplo, visualize o arquivo de log para um dos componentes do gerenciador de transações, emita o seguinte comando:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager -f
```

Para visualizar o arquivo de log para o trabalhador do gerenciador de transações, emita o comando a seguir:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager-worker -f
```

Para visualizar o arquivo de log para o componente do controlador, emita o comando a seguir:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-controller/ {print $1;exit}') -n baas -f
```

Para visualizar o arquivo de log para o componente do planejador, emita o seguinte comando:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f
```

Dica: Para ajudar a acelerar a exibição de arquivos de log, é possível incluir o sinalizador **--since=duration** no comando **kubectl logs** para retornar apenas logs que são mais recentes do que uma duração relativa. É possível especificar a duração em segundos (Ns), minutos (Nm) ou horas (Nh).

Por exemplo, para visualizar os arquivos de log para o componente do planejador com menos de 3 horas, emita o comando a seguir:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f --since=3h
```

Resolução de problemas com tarefas de backup de captura instantânea

Se uma operação de backup de captura instantânea for malsucedida, você pode tomar uma série de ações para diagnosticar o problema.

Antes de você começar, assegure-se de que o nível de rastreo esteja configurado como DEBUG. Para obter instruções sobre como configurar o nível de rastreo de arquivos de log, consulte [“Configurando o nível de rastreo de arquivos de log” na página 535](#).

Complete as etapas a seguir para solucionar problemas de backup de captura instantânea:

1. Assegure-se de que os arquivos de log do Suporte de Backup de Kubernetes estejam disponíveis. Para obter instruções sobre como visualizar os arquivos de log, consulte [“Visualizando Arquivos de Log” na página 542](#).
2. Se IBM Spectrum Protect Plus estiver enviando a solicitação de captura instantânea, verifique o log do contêiner baas-transaction-manager no pod baas-transaction-manager. No arquivo de log, procure por texto que seja semelhante ao exemplo a seguir:

```
/createvolumesnapshot/demo/demo-vol01 Begin
Received parameters {'metadata.name': 'k8s18-1004-2222-1727b1c0828',
'spec.snapshotClassName':
'cirrus-csi-rbdplugin-snapclass', 'metadata.labels': {'storage.kubernetes.io/pvc': 'demo-vol01'}}}
```

O nome da captura instantânea esperado é o valor da chave `metadata.name`.

Em seguida, procure a chamada `createsnapshot` no exemplo a seguir:

```
2020-06-03 16:55:43,579[MainThread][kubernetes_api:createsnapshot Line 1056][INFO] -
{'apiVersion':
'snapshot.storage.k8s.io/v1alpha1', 'kind': 'VolumeSnapshot', 'metadata': {'annotations':
{}}, 'name':
'k8s18-1004-2222-1727b1c0828', 'namespace': 'demo', 'labels': {'app.kubernetes.io/
component': 'snapshot',
'app.kubernetes.io/managed-by': 'baas', 'app.kubernetes.io/name': 'baas', 'app.kubernetes.io/
version': '10.1.6',
'storage.kubernetes.io/pvc': 'demo-vol01'}}}, 'spec': {'snapshotClassName': 'cirrus-csi-
rbdpugin-snapclass',
'source': {'kind': 'PersistentVolumeClaim', 'name': 'demo-vol01'}}}}
```

3. Se uma exceção for encontrada na Etapa 2, você pode encontrar a seguinte exceção na chamada `createsnapshot`.

Tabela 67. Possível exceção de backup de captura instantânea	
Exceção	Ação
A captura instantânea não existe. A captura instantânea pode não ser criada adequadamente.	Execute o comando a seguir para determinar se a captura instantânea foi criada corretamente: <pre>kubectl describe volumesnapshots <i>snapshotname</i> -n <i>namespace</i></pre>

4. Solucione problemas do IBM Spectrum Protect Plus executando as seguintes ações:

- Na interface com o usuário do IBM Spectrum Protect Plus, verifique se há alguma tarefa de inventário interrompida que esteja impedindo que todas as outras tarefas sejam registradas em IBM Spectrum Protect Plus.
- Procure a tarefa interrompida na lista de tarefas em execução ou no histórico da tarefa. Procure por nomes de tarefas com a seguinte convenção de nomenclatura:

```
k8s_sla_name
```

em que o `sla_name` é o nome da política de SLA que é designada ao PVC.

- Verifique os logs da tarefa e resolva quaisquer problemas relatados. Para obter informações sobre como visualizar e fazer o download de arquivos de log IBM Spectrum Protect Plus, consulte [“Visualizar Logs de Tarefa”](#) na página 333.

Faça o download do pacote de arquivos de log e expanda o pacote. O pacote transferido por download tem a seguinte convenção de nomenclatura: `JobLog_job_name_job-timestamp.zip`.

Para obter informações detalhadas sobre uma tarefa, revise os arquivos `command.log` e `JobLog_k8s_sla_name_job_timestamp.csv`.

Resolução de problemas com tarefas de backup de cópia

Se uma tarefa de backup de cópia não for bem-sucedida, será possível tomar uma série de ações para diagnosticar o problema.

Antes de começar, assegure-se de que o nível de rastreamento para arquivos de log esteja configurado como `DEBUG`. Para obter instruções sobre como configurar o nível de rastreamento de arquivos de log, consulte [“Configurando o nível de rastreamento de arquivos de log”](#) na página 535.

Conclua as etapas a seguir para solucionar problemas de backup de cópia:

- Assegure-se de que os arquivos de log do Suporte de Backup de Kubernetes estejam disponíveis. Para obter instruções sobre como visualizar os arquivos de log, consulte [“Visualizando Arquivos de Log”](#) na página 542.

2. Verifique se o agente IBM Spectrum Protect Plus está enviando uma solicitação para o planejador IBM Spectrum Protect Plus. Abra o arquivo de log do planejador e procure um texto que seja semelhante ao exemplo a seguir:

```
Schedule data copy for snapshot: demo:pvc-backup-demo-vol01-1004-1591203980176
```

A convenção de nomenclatura para o backup de cópia da PVC é:

```
namespace:pvc-backup-pvcname-jobid-job_timestamp
```

Procure a chamada para o gerenciador de transações para implementar um movedor de dados, como o exemplo a seguir:

```
url tmCopyBackupRequest: https://baas-transaction-manager:5000/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176"
```

Se o planejador não estiver enviando pedidos de backup de cópia, investigue e resolva as questões do planejador.

3. Se o planejador estiver enviando a solicitação de captura instantânea, verifique o log do contêiner baas-transaction-manager no pod baas-transaction-manager. No arquivo de log do gerenciador de transações, procure a chamada do movedor de dados de criação no texto que é semelhante ao exemplo a seguir:

```
/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176 method=POST
2020-06-03 17:11:26,455[MainThread][main:createdatamover Line 1187][DEBUG] - Creating deployment backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:pvc-backup-demo-vol01-1004-1591203980176
```

No log baas-transaction-manager-worker no pod baas-transaction-manager, o início da solicitação mostra o ID da tarefa, a solicitação COPYBACKUP, o nome da implementação ou o nome do movedor de dados e o nome do volume:

```
2020-06-03 17:11:26,589: DEBUG/MainProcess] TaskPool: Apply <function _fast_trace_task at 0x7ff1707ac268> (args:('main.backgroundprocess', '29606e23-b6e3-4965-8156-930b42c12a25', {'lang': 'py', 'task': 'main.backgroundprocess', 'id': '29606e23-b6e3-4965-8156-930b42c12a25', 'shadow': None, 'eta': None, 'expires': None, 'group': None, 'retries': 0, 'timelimit': [None, None], 'root_id': '29606e23-b6e3-4965-8156-930b42c12a25', 'parent_id': None, 'argsrepr': '({ 'COPYBACKUP', {'command': 'backup', 'namespace': 'demo', 'deploymentName': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176', 'volumename': 'pvc-backup-demo-vol01-1004-1591203980176', 'vSnapIPAddresses': ['9.11.62.84'], 'vSnapMountPath': '/vsnap/vpool1/fs489', 'kafkaAddress': 'baas-kafka-svc.baas:9092', 'kafkaStatusLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-status', 'kafkaCommandLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-command', 'storageClass': None, 'sizeInBytes': None, 'pvclabels': {}})', 'kwargsrepr': '{}', 'origin': 'gen28@baas-transaction-manager-69cffc84fd-95kc4', 'reply_to': '38ff7ee8-718f-3b14-bd70-8a3f866823f6', 'correlation_id':... kwargs:{}) [2020-06-03 17:11:26,593: DEBUG/MainProcess] Task accepted: main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] pid:24

Create datamover demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176 PVC=pvc-backup-demo-vol01-1004-1591203980176 isBackup=True

[2020-06-03 17:11:27,127: INFO/ForkPoolWorker-1] Task main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] succeeded in 0.5342374939937145s: 0
```

No log do gerenciador de transações, a instrução de rastreamento a seguir mostra se a implementação foi bem-sucedida ou falhou com a chamada Get deployment:

```
Get deployment backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176
```

4. No log do planejador, verifique se um backup de cópia foi concluído procurando por rastreios que sejam semelhantes aos exemplos a seguir:

```
copyBackup volume:demo:pvc-backup-demo-vol01-1004-1591203980176 jobInfoId=1004
ipAddr=[9.11.62.84] fileLocation= volumeSize=1073.741824 nextRunTime=1591290380176 "
```

Setting backup to complete for copyBackup: demopvc-backup-demo-vol01-1004-1591203980176:1591203980176

5. Se uma exceção for encontrada, você pode encontrar as exceções a seguir na solicitação COPYBACKUP.

Tabela 68. Possíveis exceções de backup de cópia	
Exceção	Ação
A captura instantânea não existe. A captura instantânea pode não ser criada adequadamente.	Execute o comando a seguir para determinar se a captura instantânea foi criada corretamente: <pre>kubectl describe volumesnapshots <i>snapshotname</i> -n <i>namespace</i></pre>
A implementação não existe. O movedor de dados pode não ser criado corretamente.	Para obter mais informações sobre o assunto, obtenha o nome do movedor de dados a partir da mensagem de erro e execute o seguinte comando: <pre>kubectl describe deploy backup-pvcname-jobname-job_timestamp -n <i>namespace</i></pre>

6. Solucione problemas do IBM Spectrum Protect Plus executando as seguintes ações:
- Na interface com o usuário do IBM Spectrum Protect Plus, verifique se há alguma tarefa de inventário interrompida que esteja impedindo que todas as outras tarefas sejam registradas em IBM Spectrum Protect Plus.
 - Procure a tarefa interrompida na lista de tarefas em execução ou no histórico da tarefa. Procure por nomes de tarefas com a seguinte convenção de nomenclatura:

```
k8s_sla_name
```

em que o *sla_name* é o nome da política de SLA que é designada ao PVC.

- Verifique os logs da tarefa e resolva quaisquer problemas relatados. Para obter informações sobre como visualizar e fazer o download de arquivos de log IBM Spectrum Protect Plus, consulte [“Visualizar Logs de Tarefa” na página 333](#).

Faça o download do pacote de arquivos de log e expanda o pacote. O pacote transferido por download tem a seguinte convenção de nomenclatura: `JobLog_job_name_job_timestamp.zip`.

Para obter informações detalhadas sobre uma tarefa, revise os arquivos `command.log` e `JobLog_k8s_sla_name_job_timestamp.csv`.

Resolução de problemas de tarefas de restauração

Se uma tarefa de restauração não for bem-sucedida, você pode tomar as seguintes ações para diagnosticar o problema.

Antes de você começar, assegure-se de que o nível de rastreamento esteja configurado como DEBUG. Para obter instruções sobre como configurar o nível de rastreamento de arquivos de log, consulte [“Configurando o nível de rastreamento de arquivos de log” na página 535](#).

Conclua as etapas a seguir para solucionar problemas de tarefa de restauração:

- Assegure-se de que os arquivos de log do Suporte de Backup de Kubernetes estejam disponíveis. Para obter instruções sobre como visualizar os arquivos de log, consulte [“Visualizando Arquivos de Log” na página 542](#).

2. Verifique se há erros no log da tarefa de restauração do servidor IBM Spectrum Protect Plus denominado `onDemandRestore_timestamp`.

Se a tarefa de restauração foi iniciada a partir da linha de comandos **kubectl**, será possível localizar o nome da tarefa de restauração nos objetos BaasReq enquanto a tarefa de restauração estiver em andamento emitindo o seguinte comando:

```
kubectl describe baasreq restore_request_name -n namespace | grep Inprogress
```

Procure por uma saída que seja semelhante ao exemplo a seguir:

```
Inprogress: onDemandRestore_1591384200276
```

3. Se você restaurou dados da linha de comandos **kubectl**, verifique se a solicitação de restauração foi invalidada devido a parâmetros inválidos no arquivo de configuração YAML. Use o comando **kubectl describe** para verificar o status de restauração (`Restorestatus`) na saída.

Se o valor no campo `Restorestatus` for `Invalid`, o campo `Errmsg` mostrará a razão pela qual o pedido de restauração foi invalidado. No exemplo a seguir, um valor incorreto foi especificado no parâmetro **VolumeStorageClass** no arquivo YAML.

Por exemplo, para mostrar o status de restauração da solicitação de restauração `copy-restore-pvc02` no espaço de nomes `test`, emita o comando a seguir:

```
kubectl describe baasreq copy-restore-pvc02 -n test
```

A saída é semelhante ao seguinte exemplo:

```
Name:          copy-restore-pvc02
Namespace:     test
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  None
Errmsg:        VolumeStorageClass invalid
Kind:          BaaSReq
Metadata:
  Creation Timestamp:  2020-06-05T19:51:29Z
  Generation:         2
  Resource Version:    4396987
  Self Link:           /apis/baas.io/v1alpha1/namespaces/test/baasreqs/copy-restore-pvc02
  UID:                418cc8d5-7347-47ed-9436-9fe49f69b42a
Restorestatus:  Invalid
Spec:
  Inprogress:      None
  Origreqtype:     restore
  Pvcname:         pvc02
  Requesttype:     restore
  Restorepoint:    2020-06-05 17:22:35
  Restoretype:     copy
  Storageclass:    cirrus19-csi-rbd-sc
  Targetvolume:    pvc02-restored
  Volumename:      pvc02
  Events:          <none>
```

Para recuperar-se desse tipo de erro, exclua a solicitação de restauração inválida, corrija o arquivo YAML e recrie a solicitação de restauração.

4. Revise as mensagens de erro no log IBM Spectrum Protect Plus do servidor `onDemandRestore_timestamp`. As mensagens de erro geralmente são suficientes para ajudá-lo a diagnosticar o problema.
5. Para solucionar mais problemas de restauração de uma captura instantânea, é possível procurar por rastreios no log da tarefa `baas-spp-agent` do agente de aplicativo que sejam semelhantes ao exemplo a seguir:

```
DEBUG pid:3402 MainThread restoreDatabase: Starting restore of snapshot
spp-1275-2213-17285db4b80 to test-snap-restore-pvc1
DEBUG pid:3402 MainThread restoreDatabase: Restoring pvc labels {'department': 'sales',
'team': 'green'}
DEBUG pid:3402 MainThread restoreDatabase: Restoring snapshot named spp-1275-2213-17285db4b80
```



```
DEBUG pid:3402 MainThread sendRestoreRequest: Sending restore request to https://baas-transaction-manager:5000/restorevolumebackup/test/test-snap-restore-pvc1?storageclass=cirrus-csi-rbd-sc&restoretype=FAST
DEBUG pid:3402 MainThread sendRestoreRequest: Get restore response
```

Verifique o log do contêiner `baas-transactionmanager` no pod `baas-transaction-manager`. No arquivo de log, procure pelo texto que seja semelhante ao exemplo a seguir:

```
/restorevolumebackup/test/test-snap-restore-pvc1 snapshot:spp-1275-2213-17285db4b80
restoretype:FAST
storageclass: cirrus-csi-rbd-sc
```

6. Para resolver ainda mais a restauração de cópia, é possível procurar por rastreios no log da tarefa `baas-spp-agent` do agente de aplicativo que sejam semelhantes ao exemplo a seguir:

```
JOBLOG_SUMMARY pid:4219 MainThread jobsummary: <CTGGK3005> Starting to restore a persistent volume.
DEBUG pid:4219 MainThread copyRestore: Starting restore of database cirrus19:test:pvc02
DEBUG pid:4219 MainThread getPVC: PVC test:test-copy-restore-pvc02 not found.
DEBUG pid:4219 MainThread copyRestore: PVC does not exist, the restore can continue.
DEBUG pid:4219 MainThread createDatamover: PVC labels {'department': 'sales', 'team': 'green'}
INFO pid:4219 MainThread createDatamover: Create datamover request to https://baas-transaction-manager:5000/datamover/test/test-copy-restore-pvc02
```

Verifique o log do contêiner `baas-transactionmanager` no pod `baas-transaction-manager`. No arquivo de log, procure pelo texto que seja semelhante ao exemplo a seguir:

```
main:createdatamover Line 1187][DEBUG] - Creating deployment
restore-pvc02-ondemandrestore-1591390864757-1591390865107 for PVC test:test-copy-restore-pvc02
```

No arquivo de log `transaction-manager-worker`, procure por um texto que seja semelhante ao exemplo a seguir:

```
DEBUG/ForkPoolWorker-1] Restore worker
DEBUG/ForkPoolWorker-1] Create datamover test:restore-pvc02-ondemandrestore-1591390864757-1591390865107
PVC=test-copy-restore-pvc02 isBackup=False
```

Tarefas relacionadas

[“Configurando o nível de rastreo de arquivos de log” na página 535](#)

É possível configurar o nível de rastreo de arquivos de log locais para ajudar a solucionar problemas que você pode encontrar no Suporte de Backup de Kubernetes.

Referências relacionadas

[“Resolução de problemas de referência rápida” na página 537](#)

Soluções para problemas básicos do Suporte de Backup de Kubernetes são fornecidas.

Capítulo 21. 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.

Tabela 69. Prefixos de mensagens por componente	
Prefixo	Componente
CTGGA	IBM Spectrum Protect Plus
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
CTGGK	IBM Spectrum Protect Plus para Contêineres
CTGGL	IBM Spectrum Protect Plus para Amazon EC2
CTGGR	IBM Spectrum Protect Plus para o Microsoft Office 365
CTGGT	IBM Spectrum Protect Plus para sistemas de arquivos

Para obter uma lista de todas as mensagens, consulte o IBM Knowledge Center [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/) (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-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
IBM Corporation
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
IBM Corporation
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.

A marca registrada Linux é usada conforme uma sublicença da Linux Foundation, a licenciada exclusiva de Linus Torvalds, proprietário da marca em nível mundial.

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 em 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

Há um glossário disponível com termos e definições para a família de produtos IBM Spectrum Protect. Consulte o [IBM Spectrum Protectglossário](#).

Índice Remissivo

A

- acesso de usuário [10](#), [517](#)
- acordo de nível de serviço, *Veja* Políticas de SLA
- acordos de nível de serviço
 - Suporte de Backup de Kubernetes [319](#)
- Amazon EC2
 - contas
 - incluindo [290](#)
 - detectando recursos [291](#)
 - tarefa de backup, criando [291](#)
 - usuário do IAM, criando [288](#)
- ambientes virtuais [199](#), [200](#)
- armazenamento de backup
 - opções avançadas, gerenciando [122](#)
 - opções de armazenamento, gerenciando discos [118](#)
 - opções de armazenamento, gerenciando parceiros [120](#)
- Armazenamento de Objeto
 - Amazon S3 [184](#)
- Arquivamento de log
 - Db2 [376](#)
- arquivos
 - pesquisando por [551](#)
 - restauração [296](#)
- arquivos de log de implementaçãoSuporte de Backup de Kubernetes [534](#)
- arquivos de log do O365
 - Detalhado [360](#)
- arquivos YAML
 - Suporte de Backup de Kubernetes [336](#)
- ativar rastreo
 - Suporte de Backup de Kubernetes [535](#)
- Atualização
 - servidor vSnap [176](#)
- atualizações de disponibilidade antecipada, obtendo e aplicando [182](#)
- atualizações off-line [178](#)
- atualizações online [178](#)
- AWS EC2
 - tarefa de restauração, criando [293](#)

B

- backup de captura instantânea
 - contêineres [340](#)
 - Suporte de Backup de Kubernetes [338](#)
- backup de cópia
 - Suporte de Backup de Kubernetes [338](#)
- Backup de log do Db2 [376](#)
- backup on demand
 - contêineres [340](#)
- backup por rótulo
 - Suporte de Backup de Kubernetes [342](#)
- backup-by-namespaces
 - Suporte de Backup de Kubernetes [345](#)
- backups de captura instantânea
 - Kubernetes [325](#)

- backups de cópia
 - Kubernetes [325](#)

C

- Centro de Operações do IBM Spectrum Protect
 - Acessando por meio do IBM Spectrum Protect Plus [16](#)
 - Incluindo o IBM Spectrum Protect Plus em [17](#)
 - iniciando a partir do IBM Spectrum Protect Plus [20](#)
 - Monitorando o IBM Spectrum Protect Plus por meio de [16](#), [20](#)
 - URL, configuração [19](#)
- certificado
 - excluindo [212](#)
 - incluindo [212](#)
- Certificado SSL, fazendo upload
 - a partir do console administrativo [214](#)
- chave
 - excluindo [211](#), [214](#)
 - incluindo [211](#), [212](#)
- chaves [211](#)
- cliente de objeto [199](#), [200](#)
- coletando arquivos de log de depuraçãoSuporte de Backup de Kubernetes [534](#)
- comando DEFINE STGPOOL [193](#)
- Configuração da rede [119](#)
- Configurando Armazenamento de Backup
 - opções de armazenamento, incluindo discos [119](#)
- configurando em Kubernetes
 - Suporte de Backup de Kubernetes [152](#)
- configurando níveis de rastreo
 - Suporte de Backup de Kubernetes [535](#)
- Configurando o Db2
 - Opções de SLA [375](#)
- conjunto de armazenamentos de cache de dados frios [193](#)
- Console Administrativo, efetuando logon no [210](#)
- Controle de Acesso
 - MongoDB [434](#)
- cópia de dados para fita
 - configurando [193](#)
- copiando dados para fita [193](#)
- criação
 - funções [523](#)
 - grupos de recursos [518](#)
 - Políticas de SLA [236](#), [241](#), [242](#)
 - Proxies VADP [260](#)
 - relatórios [515](#)
 - usuários
 - grupo LDAP [526](#)
 - individual [526](#)
- criando um segredo de extração de imagem
 - Suporte de Backup de Kubernetes [149](#)

D

- data protection [200](#)
- Db2

Db2 (*continuação*)
 requisitos do sistema [60](#)
definindo backups do SLA
 Kubernetes [325](#)
demo
 site [229](#)
 SLA [229](#)
 vSnap [229](#)
Desinstalando o
 Suporte de Backup de Kubernetes [157](#)
destruindo backupsSuporte de Backup de Kubernetes [353](#)
Detectando
 Db2 [368](#)
 Recursos do sistema de arquivos [302](#)
Dispositivo virtual
 atualizando o [178](#)
Dispositivo Virtual
 acesso
 no Hyper-V [216](#)
 no VMware [216](#)
 incluindo capacidade de armazenamento [220](#)
 incluindo um disco para [219](#)
 instalando
 no Hyper-V [101](#)
 no VMware [99](#)
Dispositivo virtual vCenter baseado no Linux, fazendo
backup [259](#)

E

editando
 configurações [209](#)
 funções [525](#)
 grupos de recursos [521](#)
 identidades [528](#)
 Políticas de SLA [247](#)
 Servidor LDAP [209](#)
 Servidor SMTP [209](#)
 sites [205](#)
 tarefas e planejamentos de tarefas [501](#)
 usuários [527](#)
efix [182](#)
Exchange Server
 requisitos do sistema [66](#)
excluindo
 demo [229](#)
 demo de SLA [247](#)
 funções [526](#)
 grupos de recursos [521](#)
 identidades [529](#)
 Políticas de SLA [247](#)
 Servidor LDAP [210](#)
 Servidor SMTP [210](#)
 sites [206](#)
 tarefas [502](#)
 usuários [528](#)
excluindo backups
 Suporte de Backup de Kubernetes [353](#)
executando relatórios
 tarefas de backup do contêiner [333](#)
executar backup
 dados do contêiner [338](#)
expirar sessão de tarefa [492](#)

F

Fazendo backup
 dados do sistema de arquivos [304](#)
 Db2 [370](#)
fazendo backup de dados do contêiner
 on demand [340](#)
 planejamento [325](#), [338](#)
 por espaço de nomes [345](#)
 por rótulo [342](#)
firewalls [104](#)
funções
 criação [523](#)
 editando [525](#)
 excluindo [526](#)
 tipos de permissão [523](#)
funções de usuários
 Suporte de Backup de Kubernetes [320](#)
fuso horário, configuração [215](#)

G

Gerenciador Ops
 MongoDB [438](#)
gerenciando tarefas
 backups e restaurações de contêiner [350](#)
grupos de recursos
 criação [518](#)
 editando [521](#)
 excluindo [521](#)
 tipos de [519](#)

H

host local
 vSnap [229](#)
Hyper-V
 Dispositivo Virtual
 acesso [216](#)
 incluindo [275](#)
 instalando no dispositivo virtual [101](#)
 servidores
 ativando o WinRM [276](#)
 detectando recursos para [277](#)
 testando a conexão com [277](#)
 tarefa de backup, criando [277](#)
 tarefa de restauração, criando [281](#)

I

IBM Knowledge Center [ix](#)
identidades
 editando [528](#)
 excluindo [529](#)
 incluindo [528](#)
implementando em Kubernetes
 Suporte de Backup de Kubernetes [152](#)
incapacidade [553](#)
incluindo
 conta do Amazon EC2 [290](#)
 discos virtuais para uma máquina virtual vCenter [219](#)
 identidades [528](#)
 Instâncias do vCenter Server [249](#)

- incluindo (*continuação*)
 - Servidor LDAP [207](#)
 - Servidor SMTP [208](#)
 - servidores de aplicativos Oracle [462](#)
 - Servidores de aplicativos SQL Server [475](#)
 - servidores Hyper-V [275](#)
 - servidores vSnap [115](#)
 - sites [204](#)
- Incluindo Db2 [367](#)
- Incluindo o MongoDB [436](#)
- Incluindo um sistema de arquivos [300](#)
- Incluir Partições Db2 [367](#)
- iniciação rápida [159](#)
- iniciando
 - IBM Spectrum Protect Plus [161](#)
 - tarefas
 - no planejamento [236](#), [241](#), [242](#)
 - on demand [497](#)
- instalando
 - Dispositivo Virtual
 - no Hyper-V [101](#)
 - no VMware [99](#)
 - pacotes de download, obtendo [98](#)
 - servidores vSnap
 - ambiente de VMware [110](#)
 - ambiente do Hyper-V [112](#)
 - ambiente físico [109](#)
 - Suporte de Backup de Kubernetes [149](#)
- instalando em Kubernetes
 - Suporte de Backup de Kubernetes [152](#)
- inventário
 - sistemas de arquivos [302](#)

K

- Knowledge Center [ix](#)
- Kubernetes
 - clusters
 - modificar propriedades [322](#)
 - registrando manualmente [322](#)
- Kubernetes Cluster
 - detectando recursos [325](#)
 - testando a conexão com [325](#)

L

- LDAP
 - grupo, criando uma conta do usuário para [526](#)
 - server
 - configurações, editando [209](#)
 - excluindo [210](#)
 - incluindo [207](#)
- Localizando o Db2 [368](#)
- Localizando unidades do sistema de arquivos [302](#)
- logs
 - auditoria
 - fazendo download [516](#)
 - visualizando [516](#)
 - system
 - fazendo download [533](#)
 - visualizando [533](#)
- logs de processo detalhados
 - O365 [360](#)

M

- mensagem
 - prefixos [549](#)
- mensagens [549](#)
- modificando propriedades
 - Clusters do Kubernetes [322](#)
- MongoDB
 - requisitos do sistema [72](#)
- monitoramento
 - tarefas de backup do contêiner [333](#)

N

- NICs [119](#)
- Novo no IBM Spectrum Protect Plus Versão Versão 10.1.6 [xi](#)

O

- ocupação variada
 - Suporte de Backup de Kubernetes [317](#), [321](#)
- Office [365](#) [357](#)
- Opções de backup advanced [122](#)
- Opções de SLA
 - Db2 [375](#)
- Operations Center
 - Acessando por meio do IBM Spectrum Protect Plus [16](#)
 - Incluindo o IBM Spectrum Protect Plus em [17](#)
 - iniciando a partir do IBM Spectrum Protect Plus [20](#)
 - Monitorando o IBM Spectrum Protect Plus por meio de [16](#), [20](#)
 - URL, configuração [19](#)
- Oracle
 - bancos de dados multienclavados [462](#)
 - requisitos do sistema [82](#)
 - servidores de aplicativos
 - detectando recursos para [464](#)
 - incluindo [462](#)
 - testando a conexão com [464](#)
 - tarefa de backup, criando [464](#)
 - tarefa de restauração, criando [467](#)

P

- Parceiros de replicação [120](#)
- planejando backups
 - Kubernetes [325](#)
 - Suporte de Backup de Kubernetes [338](#)
- Planejar tarefas
 - Backup [372](#), [395](#), [442](#)
- políticas de backup, *Veja* Políticas de SLA
- Políticas de SLA
 - editando [247](#)
 - excluindo [247](#)
 - incluindo [236](#), [241](#), [242](#)
 - Suporte de Backup de Kubernetes [319](#), [338](#)
- pontos de restauração, excluindo [493](#)
- pontos de restauração, gerenciando [492](#)
- pré-requisito
 - Db2 [363](#)
 - MongoDB [433](#)
 - sistemas de arquivos [299](#)
 - Suporte de Backup de Kubernetes [149](#)

- Pré-requisitos
 - MongoDB [434](#)
- preferências
 - global
 - configurando [222](#)
- preferências globais
 - configurando [222](#)
- Programa beta
 - vantagens [xiii](#)
 - visão geral geral [xiii](#)
- programa do usuário patrocinador
 - vantagens [xiii](#)
 - visão geral geral [xiii](#)
- proteção de dados [199](#)
- provedor do servidor de repositório
 - editando [204](#)
 - excluindo [204](#)
- provedor em nuvem
 - editando [190](#)
 - excluindo [190](#)
- Proxies VADP
 - atualizando o [181](#)
 - criação [260](#)
 - opções, configurando [263](#)
 - removendo a instalação [264](#)
- publicações [ix](#)

R

- RBAC
 - MongoDB [434](#)
- recuperação do vSnap [129](#)
- recurso volumeSnapshotDataSource
 - Suporte de Backup de Kubernetes [149](#)
- recursos de acessibilidade [553](#)
- recursos de segurança
 - Suporte de Backup de Kubernetes [321](#)
- rede
 - testando [217](#), [218](#)
- rede fenced, criando [271](#)
- reexecutar
 - tarefas
 - on demand [502](#)
- registrando
 - Clusters do Kubernetes [322](#)
 - servidores vSnap [115](#)
- registrando manualmente
 - Clusters do Kubernetes [322](#)
- relatórios
 - customizado, criando [515](#)
 - executando
 - no planejamento [515](#)
 - on demand [514](#)
 - executando VM [512](#)
 - tipos de
 - proteção [508](#)
 - system [511](#)
 - utilização de armazenamento de backup [507](#)
- remoção
 - demo [229](#)
- removendo atribuições de política do SLA
 - Kubernetes [325](#)
- reparar vSnap [129](#)
- requisitos do sistema

- requisitos do sistema (*continuação*)
 - componentes [23](#)
 - Db2 [60](#)
 - Exchange Server [66](#)
 - hypervisores [40](#)
 - índice de arquivo e restauração [43](#)
 - MongoDB [72](#)
 - Oracle [82](#)
 - sistemas de arquivos [50](#)
 - SQL Server [90](#)
 - Suporte de Backup de Kubernetes [54](#)
- resolução de problemas
 - exibindo logs do Suporte de Backup de Kubernetes [541](#)
 - Operações do Suporte de Backup de Kubernetes [541](#)
 - Suporte de Backup de Kubernetes [534](#)
- restauração de captura instantânea
 - volumes persistentes [329](#)
- restauração de cópia
 - dados do contêiner [348](#)
 - volumes persistentes [329](#)
- restauração rápida
 - dados do contêiner [348](#)
- Restaurando
 - Db2 [377](#), [383](#), [386](#)
 - sistema de arquivos [310](#)
- restaurando dados [329](#)
- restaurando dados do contêiner
 - Suporte de Backup de Kubernetes [348](#)
- Restaurando o Db2
 - Instância alternativa [386](#)
 - Instância original [383](#)
- restaurando volumes persistentes
 - Kubernetes [329](#)
- restaurar tarefas
 - criação
 - AWS EC2 [293](#)
 - Hyper-V [281](#)
 - IBM Spectrum Protect Plus [491](#)
 - Oracle [467](#)
 - SQL Server [481](#)
 - VMware [264](#)
 - executando
 - AWS EC2 [293](#)
 - Hyper-V [281](#)
 - Oracle [467](#)
 - SQL Server [481](#)
 - VMware [264](#)
- retenção de captura instantânea [492](#)

S

- scripts para operações de backup e restauração
 - fazendo upload [504](#)
- servidor de aplicativos
 - Db2 [363](#)
- Servidor de aplicativos MongoDB [433](#)
- servidor de armazenamento de backup
 - opções de armazenamento, gerenciando [119](#), [121](#)
- Servidor de proteção de espectro IBM
 - incluindo um servidor de repositório [202](#)
 - registrando um servidor de repositório [202](#)
- servidor em nuvem
 - incluindo um Amazon S3 [184](#)
 - incluindo um recurso de nuvem compatível com s3 [188](#)

- servidor em nuvem (*continuação*)
 - incluindo um recurso de nuvem Microsoft azure [187](#)
 - incluindo um recurso do IBM Cloud Object Storage [185](#)
- servidor vSnap
 - administrando
 - administração de armazenamento [131](#)
 - administração de rede [134](#)
 - administração de usuário [130](#)
 - cabeçalhos do kernel
 - ferramentas do kernel [135](#)
 - Cancelando o Registro [116](#)
 - conjuntos de armazenamentos, expandindo [128](#)
 - editando [116](#)
 - inicializando
 - avançado [127](#)
 - simple [127](#)
 - mudar rendimento [128](#)
- servidores vSnap
 - incluindo [115](#)
 - instalando
 - ambiente de VMware [110](#)
 - ambiente do Hyper-V [112](#)
 - ambiente físico [109](#)
 - registrando [115](#)
 - removendo a instalação [113](#)
- sistemas de arquivos
 - requisitos do sistema [50](#)
- sites
 - editando [205](#)
 - excluindo [206](#)
 - incluindo [204](#)
 - regulador [204](#), [205](#)
- SLA [372](#), [395](#), [442](#)
- SMTP
 - server
 - configurações, editando [209](#)
 - excluindo [210](#)
 - incluindo [208](#)
- SQL Server
 - requisitos do sistema [90](#)
 - requisitos para proteção de dados [474](#)
 - servidores de aplicativos
 - detectando recursos para [477](#)
 - incluindo [475](#)
 - testando a conexão com [477](#)
 - tarefa de backup, criando [477](#)
 - tarefa de restauração, criando [481](#)
- Suporte de Backup de Kubernetes
 - ações em cascata [149](#)
 - Arquivo de configuração [152](#)
 - ativar rastreo [535](#)
 - ativar recurso VolumeSnapshotDataSource [149](#)
 - backup de captura instantânea [338](#), [340](#)
 - backup de cópia [338](#)
 - backup por rótulo [342](#)
 - backup-by-namespace [345](#)
 - coletando arquivos de log de depuração [534](#)
 - configurando níveis de rastreo [535](#)
 - criando um segredo de extração de imagem [149](#)
 - encryption [321](#)
 - excluindo backups [353](#)
 - executando relatórios [333](#)
 - exibindo arquivos de log [541](#)
 - fazendo backup de dados do contêiner [338](#)

- Suporte de Backup de Kubernetes (*continuação*)
 - fazendo backup de PVCs por espaço de nomes [345](#)
 - fazendo backup de PVCs por rótulo [342](#)
 - funções de usuários [320](#)
 - gerenciando tarefas [350](#)
 - instalando [149](#)
 - instalando em Kubernetes [152](#)
 - logs de implementação [534](#)
 - monitorando tarefas [333](#)
 - ocupação variada [321](#)
 - planejando backups [338](#)
 - Políticas de SLA [319](#), [338](#)
 - pré-requisito [149](#)
 - remoção da instalação [157](#)
 - requisitos do sistema [54](#)
 - resolução de problemas [534](#)
 - resolução de problemas de tarefas de backup [541](#)
 - resolução de problemas de tarefas de restauração [541](#)
 - restauração de cópia [348](#)
 - restauração rápida [348](#)
 - restaurando dados [348](#)
 - segurança [321](#)
 - solicitação destroy [353](#)
 - solicitações baas [336](#)
 - status de restauração [352](#)
 - status do backup [352](#)
 - tarefas expiradas [332](#)
 - tipos de backup e restauração [318](#)
 - tipos de solicitações [336](#)
 - verificando o Metrics Server [149](#)
 - visão geral geral [317](#)
 - visualizando logs da tarefa [333](#)
 - visualizando logs de rastreo [536](#)
 - visualizando o histórico de backup [334](#)
 - visualizando o status de restauração [351](#)
 - visualizando o status do backup [351](#)

T

- tarefas
 - cancelando [502](#)
 - criação [496](#)
 - editando [501](#)
 - excluindo [502](#)
 - iniciando
 - no planejamento [236](#), [241](#), [242](#)
 - on demand [497](#)
 - liberando [501](#)
 - logs
 - fazendo download [500](#)
 - visualizando [500](#)
 - nomes de [495](#)
 - pausando [501](#)
 - planejamentos, editando [501](#)
 - progresso, visualizando [499](#)
 - reexecutar [502](#)
 - simultânea, visualização [500](#)
 - tipos de [495](#)
 - visualizando [498](#)
- tarefas ad hoc
 - criação [503](#)
- tarefas de backup
 - criação
 - Amazon EC2 [291](#)

- tarefas de backup (*continuação*)
 - criação (*continuação*)
 - Hyper-V [277](#)
 - IBM Spectrum Protect Plus [491](#)
 - Oracle [464](#)
 - SQL Server [477](#)
 - VMware [253](#)
 - excluindo VMDKs de [258](#)
 - iniciando
 - no planejamento [236](#), [241](#), [242](#)
 - on demand [497](#)
 - reexecutar
 - on demand [502](#)
- Tarefas e Operações [495](#)
- tarefas expiradas
 - Suporte de Backup de Kubernetes [332](#)
- teclado [553](#)
- Testando a conexão
 - Db2 [369](#)
- Testando a conexão sistemas de arquivos [303](#)
- tipos de backup
 - Suporte de Backup de Kubernetes [318](#)
- tipos de restauração
 - Suporte de Backup de Kubernetes [318](#)
- tipos de solicitações
 - Suporte de Backup de Kubernetes [336](#)

U

- usuários
 - editando [527](#)
 - excluindo [528](#)
 - funções
 - criação [523](#)
 - editando [525](#)
 - excluindo [526](#)
 - tipos de permissão [523](#)
 - grupo LDAP, criando [526](#)
 - grupos de recursos
 - criação [518](#)
 - editando [521](#)
 - excluindo [521](#)
 - tipos de [519](#)
 - indivíduo, criando [526](#)
- utilitários iSCSI
 - instalando [106](#)

V

- verificando o Metrics Server
 - Suporte de Backup de Kubernetes [149](#)
- visão geral geral
 - Suporte de Backup de Kubernetes [317](#)
- visualizando logs da tarefa
 - backups de contêiner [333](#)
- visualizando logs de rastreamento
 - Suporte de Backup de Kubernetes [536](#)
- visualizando o histórico de backup
 - backups de contêiner [334](#)
- visualizando o status de restauração
 - Suporte de Backup de Kubernetes [351](#), [352](#)
- visualizando o status do backup
 - Suporte de Backup de Kubernetes [351](#), [352](#)

- VMware
 - Dispositivo Virtual
 - acesso [216](#)
 - instalando no dispositivo virtual [99](#)
 - Instâncias do vCenter Server
 - incluindo [249](#)
 - privilegios da máquina virtual, necessários [250](#)
 - tarefa de backup, criando [253](#)
 - tarefa de backup, excluindo VMDKs da política de SLA [258](#)
 - tarefa de restauração
 - criando uma rede fenced [271](#)
 - tarefa de restauração, criando [264](#)
 - vCenter Server, detectando recursos [253](#)
 - vCenter Server, testando a conexão com [253](#)
- vSnap
 - atualizando o [178](#)

W

- WinRM, ativando para conexão com servidores Hyper-V [276](#)



Número do Programa: 5737-F11

Printed in USA