IBM Spectrum Protect
Versão 8.1.7

Guia da solução de disco multisite

IBM Spectrum Protect
Versão 8.1.7

Guia da solução de disco multisite

Observação:
Antes de utilizar essas informações e o produto que elas suportam, leia as informações em “Aviso” na página 177.

Essa edição se aplica à versão 8, liberação 1, modificação 7 do IBM Spectrum Protect (números de produto 5725-W98, 5725-W99, 5725-X15) e a todas as liberações e modificações subsequentes, até que seja indicado de outra forma em novas edições.

Índice

Sobre esta publicação v
Quem Deve Ler este Guia v
Publicações v

O que há de novo nesta liberação . . . vii

Parte 1. Planejando uma solução de proteção de dados de disco multisite 1

Capítulo 1. Selecionando um tamanho de sistema 3

Capítulo 2. Planejando os sites 5

Capítulo 3. Requisitos do sistema para uma solução de disco multisite 7
Requisitos de Hardware 7
Requisitos de Software 9

Capítulo 4. Planilhas de planejamento 13

Capítulo 5. Planejando o armazenamento 25
Planejando as matrizes de armazenamento 25

Capítulo 6. Planejando a segurança . . 29
Planejando funções de administrador 29
Planejando comunicações seguras 30
Planejando o armazenamento de dados criptografados 30
Planejando acesso ao firewall 31

Parte 2. Implementação de disco multisite de uma solução de proteção de dados 35

Capítulo 7. Configurando o sistema . . 37
Configurando o hardware de armazenamento . . . 37
Instalando o sistema operacional do servidor . . . 37
Instalando em sistemas AIX 38
Instalando em sistemas Linux 39
Instalando em sistemas Windows 44
Configurando a E/S de caminhos múltiplos . . . 45
Sistemas AIX 45
Sistemas Linux 46
Sistemas Windows 47
Criando o ID do usuário para o servidor 48
Preparando sistemas de arquivos para o servidor . . 49
Sistemas AIX 49
Sistemas Linux 50
Sistemas Windows 51

Capítulo 8. Instalando o servidor e o Operations Center 53
Instalando em sistemas AIX e Linux 53
Instalando arquivos RPM de pré-requisito para o assistente gráfico 54
Instalando em sistemas Windows 54

Capítulo 9. Configurando o servidor e o Operations Center 57
Configurando a instância do servidor. 57
Instalando o cliente de backup-archive 58
Configurando opções para o servidor. 59
Configurando comunicações seguras com a Segurança da Camada de Transporte 60
Configurando o Operations Center 61
Protegendo as comunicações entre o Operations Center e o servidor do hub 62
Registrando a licença do produto 64
Configurando a deduplicação de dados 65
Definindo regras de retenção de dados para seus negócios 65
Definindo planejamentos para atividades de manutenção de servidor 66
Definindo planejamentos de cliente 68

Capítulo 10. Instalando e configurando clientes de backup-archive 69
Registrando e designando clientes a planejamentos 69
Instalando o serviço de gerenciamento de clientes 70
Verificando que o serviço de gerenciamento de clientes está instalado corretamente 71
Configurando o Operations Center para usar o serviço de gerenciamento de clientes 72

Capítulo 11. Configurando o segundo servidor 75
Configurando comunicações de SSL entre o servidor do hub e um servidor spoke. 75
Incluindo o segundo servidor como um spoke. . . 77
Ativando a replicação 77

Capítulo 12. Concluindo a implementação 79

Parte 3. Monitorando uma solução de disco multisite 81

Capítulo 13. Lista de verificação de monitoramento diária 83

Capítulo 14. Lista de verificação de monitoramento periódica 93

Capítulo 15. Verificando a conformidade da licença 101

Capítulo 16. Rastreando o status do sistema usando relatórios de e-mail . 103

Parte 4. Gerenciando operações para uma solução de disco multisite 105

Capítulo 17. Gerenciando o Operations Center 107
Incluindo e removendo servidores spoke 107
Incluindo um Servidor spoke 107
Removendo um servidor spoke 108
Iniciando e parando o servidor da web 109
Reiniciando o assistente de configuração inicial . . 109
Alterando o servidor do hub 110
Restaurando a configuração para o estado de pré-configuração 111

Capítulo 18. Protegendo aplicativos, máquinas virtuais e sistemas 113
Incluindo clientes 113
Selecionando o software cliente e planejando a instalação. 114
Especificando regras para backup e arquivamento de dados de cliente 115
Planejando operações de backup e archive. . . 119
Registrando clientes 120
Instalando e configurando clientes 121
Gerenciando operações do cliente 126
Avaliando erros nos logs de erros do cliente . . 127
Parando e reiniciando o client acceptor 128
Reconfigurando senhas 129
Modificando o escopo de um backup de cliente 130
Gerenciando upgrades do cliente 131
Desatribuindo um nó cliente 132
Desativando dados para liberar espaço de armazenamento 134

Capítulo 19. Gerenciando armazenamento de dados 137
Auditando um contêiner do conjunto de armazenamentos 137
Gerenciando a capacidade do inventário 138
Gerenciando o uso de memória e de processor . . 140
Ajustando atividades planejadas 141
Movendo clientes de um servidor para outro 142

Capítulo 20. Gerenciando a replicação 143
Compatibilidade de replicação. 143
Ativando a replicação de nó 143
Protegendo dados em conjuntos de armazenamentos de contêiner de diretório. 144
Modificando configurações de replicação 146
Configurando diferentes políticas de retenção para o servidor de origem e o servidor de destino . . . 147

Capítulo 21. Protegendo o servidor 149
Conceitos de segurança 149
Gerenciando administradores 152
Alterando requisitos de senha 153
Protegendo o IBM Spectrum Protect no sistema 154
Restringindo o acesso de usuário ao servidor 154
Limitando o acesso por meio de restrições de porta 155

Capítulo 22. Parando e iniciando o servidor. 157
Parando o Servidor 157
Iniciando o servidor para tarefas de manutenção ou reconfiguração 158

Capítulo 23. Planejando fazer upgrade do servidor 161

Capítulo 24. Preparando-se para uma indisponibilidade ou atualização do sistema 163

Capítulo 25. Implementando um plano de recuperação de desastres 165
Concluindo drills de recuperação. 165

Capítulo 26. Recuperando-se de perda de dados ou de indisponibilidades do sistema 167
Restaurando o banco de dados 169
Recuperando dados danificados de uma cópia replicada 171
Reparando conjuntos de armazenamentos 172

Parte 5. Apêndices 173

Apêndice. Recursos de Acessibilidade para a Família de Produtos IBM Spectrum Protect. 175

Aviso 177

Glossário 183

Índice Remissivo 185

Sobre esta publicação

Esta publicação fornece informações sobre como planejar, implementar, monitorar e operar uma solução de proteção de dados que usa as melhores práticas do IBM Spectrum Protect.

Quem Deve Ler este Guia

Esse guia a destinado a qualquer pessoa que está registrada como um administrador do IBM Spectrum Protect. Um único administrador pode gerenciar o IBM Spectrum Protect, ou várias pessoas podem compartilhar responsabilidades administrativas.

É necessário estar familiarizado com o sistema operacional no qual o servidor reside e com os protocolos de comunicação requeridos para o ambiente do cliente ou do servidor. Também é necessário entender as práticas de gerenciamento de armazenamento de sua organização, sobre como você está atualmente fazendo backup de arquivos da estação de trabalho e como está usando dispositivos de armazenamento.

Publicações

A família de produtos IBM Spectrum Protect inclui o 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 nesta liberação

Esta liberação do IBM Spectrum Protect introduz novos recursos e atualizações.

Para obter uma lista de novos recursos e atualizações, consulte O que há de novo.

As informações novas e alteradas nesta documentação de produto são indicadas por uma barra vertical (|) à esquerda da mudança.

Parte 1. Planejando uma solução de proteção de dados de disco multisite

Planeje uma solução de proteção de dados de disco multisite com servidores em dois sites que usam deduplicação de dados e replicação.

Métodos de implementação

É possível configurar servidores para uma solução de disco multisite nas maneiras a seguir:

Configurar servidores usando o Operations Center e comandos administrativos
É possível configurar um intervalo de sistemas de armazenamento e o software do servidor para sua solução. As tarefas de configuração são concluídas usando assistentes e opções nos comandos do Operations Center e do IBM Spectrum Protect. Para obter informações sobre como iniciar, consulte o "Planejando o roteiro".

Configurar os servidores usando scripts automatizados
Para obter orientação detalhada sobre a configuração com sistemas de armazenamento IBM Storwize específicos e usando scripts automatizados para configurar cada servidor, veja os blueprints do IBM Spectrum Protect. A documentação e os scripts estão disponíveis no IBM developerWorks em IBM Spectrum Protect Blueprints.

A documentação de blueprint não inclui etapas para instalar e configurar o Operations Center ou para configurar comunicações seguras usando a Segurança da Camada de Transporte (TLS). A replicação é configurada usando comandos após a configuração de cada servidor. Está incluída uma opção para usar o Elastic Storage Server, baseada na tecnologia IBM Spectrum Scale.

Planejando o roteiro

Planeje uma solução de disco multisite revisando o layout da arquitetura na figura a seguir e, então, concluindo as tarefas de roteiro que seguem o diagrama.

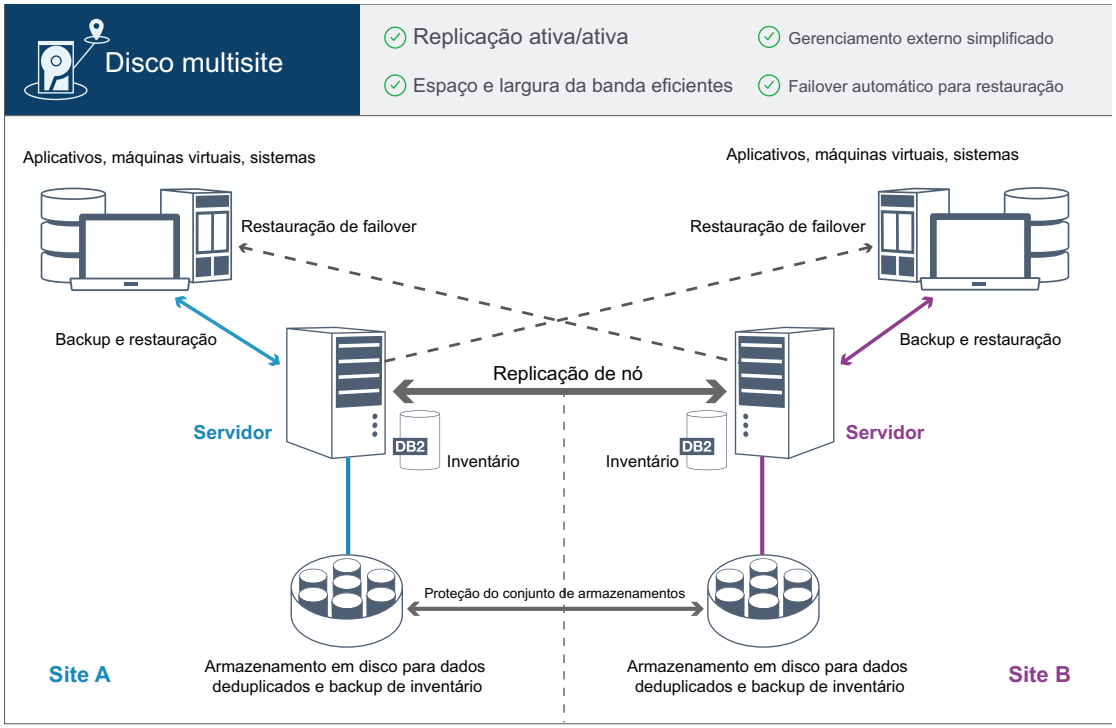


Figura 1. Solução de disco multisite

As etapas a seguir são necessárias para planejar adequadamente um ambiente de disco multisite.

1. Selecione o tamanho do seu sistema.
2. Planeje os sites.
3. Atenda aos requisitos do sistema para hardware e software.
4. Registre valores para configuração do seu sistema nas planilhas de planejamento.
5. Planeje o armazenamento.
6. Planeje a segurança.
   a. Planeje as funções de administrador.
   b. Planeje as comunicações seguras.
   c. Planeje o armazenamento de dados criptografados.
   d. Planeje o acesso ao firewall.

Capítulo 1. Selecionando um tamanho de sistema

Selecione o tamanho do servidor do IBM Spectrum Protect com base na quantidade de dados gerenciados e nos sistemas a serem protegidos.

Sobre Esta Tarefa

É possível usar as informações na tabela para determinar o tamanho do servidor que é necessário, com base na quantia de dados gerenciados.

A tabela a seguir descreve o volume de dados que um servidor gerencia. Essa quantidade inclui todas as versões. A quantidade diária de dados é a quantidade de novos dados que são submetidos a backup a cada dia. O total de dados gerenciados e a quantidade diária de novos dados são medidos como o tamanho antes de qualquer redução de dados.

Tabela 1. Determinando o tamanho do servidor

Total de dados gerenciados	**Quantidade diária de novos dados para backup**	**Tamanho do servidor necessário**
60 TB - 240 TB	Até 10 TB por dia	Pequeno
196 TB-784 TB	De 10 a 20 TB por dia	Médio
1000 TB a 4000 TB	20 a 100 TB por dia	Grande

Os valores de backup diário na tabela são baseados nos resultados do teste com objetos com 128 MB de tamanho, que são usados pelo IBM Spectrum Protect for Virtual Environments. As cargas de trabalho que consistem em objetos menores que 128 KB podem não ser capazes de atingir esses limites diários.

Capítulo 2. Planejando os sites

Revise casos de uso e avalie os fatores para fornecer a proteção de dados mais eficiente para a solução de disco multisite para o IBM Spectrum Protect.

Casos de uso

A solução de disco multisite cria pelo menos uma cópia de dados de backup. Se os servidores do IBM Spectrum Protect estiverem em locais separados, a réplica de backup será mantida externamente.

Dica: Evite conflitos no gerenciamento de IDs administrativos e de conjuntos de opções do cliente, identificando os IDs e os conjuntos de opções que serão replicados para o servidor de destino e os IDs e os conjuntos de opções que serão gerenciados em uma configuração corporativa. Não será possível definir um ID do usuário administrativo para um nó registrado se um ID administrativo existir para o mesmo nó.

Embora sua empresa possa beneficiar-se de uma solução de disco multisite por várias razões, as razões mais comuns para usar uma solução de disco multisite incluem os seguintes cenários de replicação:

A replicação do site primário para o site de recuperação de desastre

Nesse cenário, os dados que são submetidos a backup no site primário, o Site A, são replicados para um servidor no site secundário, site de recuperação de desastre, o Site B. Se ocorrer um desastre no Site A, como falha do servidor, será possível usar o servidor no Site B para recuperar sistemas. Como alternativa, é possível usar o servidor no Site A para restaurar dados do conjunto de armazenamentos primários no Site B, por exemplo, após uma falha de armazenamento em disco no Site B.

Replicação mútua em dois sites ativos

Nesse cenário, os dados locais em cada site são submetidos a backup pelos servidores no Site A e Site B. Os dados que são submetidos a backup no Site A são replicados para o Site B e os dados de backup do Site B são replicados para o Site A. Se os dados que foram submetidos a backup forem perdidos no Site A, será possível usar o servidor no Site B para recuperar dados do conjunto de armazenamentos para o servidor no Site A. Se o Site A não estiver mais disponível, será possível recuperar os dados replicados do Site A para um novo sistema no Site B. Deve-se dimensionar os recursos do servidor para assegurar que o servidor tenha capacidade suficiente para fazer backup e restaurar todos os nós clientes como parte de seu plano de recuperação de desastres.

Proteger servidores remotos no site primário

Nesse cenário, você configura servidores remotos que são relativamente pequenos para replicar dados que são submetidos a backup para um servidor maior no site primário. Se a largura da banda for limitada, pode não ser prático restaurar sistemas para os sites remotos. Nesse caso, talvez você queira recuperar sistemas no site primário antes de replicar os dados de backup para os servidores remotos.

Fatores a serem avaliados

Antes de implementar uma solução de disco multisite, avalie os seguintes fatores:

Largura da banda da rede

A rede deve ter largura da banda suficiente para as transferências de dados esperadas entre os nós, para replicação e para as operações de restauração entre sites que são necessárias para recuperação de desastre. Antes de continuar com o teste de rendimento de replicação, certifique-se de que sua rede possa manipular o tráfego de replicação. Calcule a largura da banda da rede necessária para o requisito de estado estável aplicando as diretrizes em Estimando largura da banda da rede necessária para replicação (V7.1.1).

A conexão de rede geralmente é um recurso compartilhado. Planeje o horário do dia para planejar a replicação de nó para execução para evitar um conflito com outros usuários de recursos. Além disso, os controles de rede podem limitar a atividade a somente uma parte da largura da banda. Não existem controles no IBM Spectrum Protect para restringir o uso da rede.

Recursos para a replicação inicial

Para configurar a solução de proteção de dados entre dois sites, deve-se replicar dados inicialmente do Site A para o servidor de destino no Site B. Para assegurar que a replicação inicial seja bem-sucedida, é necessário determinar se você tem a largura da banda da rede, recursos do processador e tempo disponível para replicar os dados. Pode ser necessário planejar a replicação dos backups completos iniciais por vários dias. Se não for possível estender o planejamento para os backups iniciais, é possível replicar dados do Site A par o Site B sem usar a rede. Por exemplo, é possível exportar e importar os dados de backup usando mídia ou localizar temporariamente os servidores de origem e de destino no mesmo site.

Ingestão de dados diária

Para a solução de disco multisite, a ingestão de dados diária e a retenção de dados total devem estar dentro da capacidade das configurações. Por exemplo, uma grande configuração tem uma capacidade de ingestão de dados de até 100 TB por dia, incluindo replicação de nó. Nos casos em que os requisitos de backup excedem a capacidade de um servidor único, é possível configurar uma solução que usa múltiplos servidores para atingir a capacidade necessária.

Configuração do servidor

A configuração do servidor deve atender ou exceder os requisitos da solução de disco multisite.

Réplica única de dados de backup

A solução de disco multisite é mais eficiente quando uma única cópia externa dos dados de backup atende aos requisitos de proteção de dados e de mitigação de risco. Nesse caso, a cópia única dos dados é mantida externamente no local de um servidor de replicação.

Referências relacionadas:

Capítulo 3, “Requisitos do sistema para uma solução de disco multisite”, na página 7

Capítulo 3. Requisitos do sistema para uma solução de disco multisite

Depois de selecionar a solução IBM Spectrum Protect que melhor se ajusta aos requisitos de proteção de dados, revise os requisitos do sistema para planejar a implementação da solução de proteção de dados.

Certifique-se de que seu sistema atenda aos pré-requisitos de hardware e de software para o tamanho de servidor que você planeja usar.

Informações relacionadas:

Sistemas Operacionais Suportados do IBM Spectrum Protect

Requisitos de Hardware

Os requisitos de hardware para sua solução IBM Spectrum Protect são baseados no tamanho do sistema. Escolha componentes equivalentes ou melhores que os itens que estão listados para assegurar o desempenho ideal para seu ambiente.

Para uma definição de tamanhos de sistemas, consulte Capítulo 1, “Selecionando um tamanho de sistema”, na página 3.

A tabela a seguir inclui requisitos mínimos de hardware para o servidor e armazenamento, com base no tamanho do servidor que você planeja construir. Se estiver usando partições locais (LPARs) ou partições de trabalho (WPARs), ajuste os requisitos de rede para considerar os tamanhos de partições.

Use as informações na tabela a seguir como um ponto de início. Para obter as informações mais atualizadas sobre os requisitos de hardware e as especificações para o servidor e armazenamento, veja os Blueprints do IBM Spectrum Protect.

Componente de hardware	Sistema pequeno	Sistema médio	Sistema grande
Processador do servidor	AIX 6 núcleos do processador, 3.42 GHz ou mais rápido Linux Windows 16 núcleos do processador, 1.7 GHz ou mais rápido.	AIX 10 núcleos do processador, 3.42 GHz ou mais rápido Linux Windows 20 núcleos do processador, 2.2 GHz ou mais rápido	AIX 20 núcleos do processador, 3.42 GHz Linux Windows 44 núcleos do processador, 2.2 GHz ou mais rápido
Memória do servidor	64 GB de RAM	128 GB de RAM	256 GB de RAM
Rede	• Ethernet de 10 GB (1 porta) • Adaptador Fibre Channel de 8 GB (2 portas)	• Ethernet de 10 GB (2 portas) • Adaptador Fibre Channel de 8 GB (2 portas)	• Ethernet de 10 GB (4 portas) • Adaptador Fibre Channel de 8 GB (4 portas)

Componente de hardware	Sistema pequeno	Sistema médio	Sistema grande
Armazenamento	• Discos SSD de 1,45 TB para o banco de dados, mais espaço para registros do Operations Center • Conjunto de armazenamentos de contêiner de diretório deduplicado de 67 TB	• Discos SSD de 2,53 TB para o banco de dados, mais espaço para registros do Operations Center • Conjunto de armazenamentos de contêiner de diretório deduplicado de 207,9 TB	• Discos SSD de 6,54 TB para o banco de dados, mais espaço para registros do Operations Center • Conjunto de armazenamentos de contêiner de diretório deduplicado de 1049,67 TB

Implementando a tecnologia correta de núcleo do processador

Deve-se usar o tipo correto de tecnologia de núcleo do processador para o processador do servidor. Para obter informações sobre o tipo de tecnologia de núcleo do processador, veja os Blueprints do IBM Spectrum Protect.

Estimando requisitos de espaço de banco de dados para o Operations Center

Os requisitos de hardware para o Operations Center estão incluídos na tabela anterior, exceto para o banco de dados e espaço do log de archive (inventário) que o Operations Center usa para conter registros para clientes gerenciados.

Se você não planeja instalar o Operations Center no mesmo sistema que o servidor, é possível estimar os requisitos do sistema separadamente. Para calcular os requisitos do sistema para o Operations Center, consulte a calculadora dos requisitos do sistema na nota técnica 1641684.

O gerenciamento do Operations Center no servidor é uma carga de trabalho que requer espaço extra para operações do banco de dados. A quantia de espaço depende do número de clientes que são monitorados em um servidor. Revise as diretrizes a seguir para estimar quanto espaço seu servidor requer.

Espaço de banco de dados

O Operations Center usa aproximadamente 1.2 GB de espaço de banco de dados para cada 1000 clientes que são monitorados em um servidor. Por exemplo, considere um servidor do hub com 2000 clientes que também gerencia três servidores spoke, cada um com 1500 clientes. Essa configuração tem um total de 6500 clientes entre os quatro servidores e requer aproximadamente 8,4 GB de espaço de banco de dados. Esse valor é calculado arredondando os 6500 clientes para o milhar mais próximo, que é 7000:

```
7 x 1.2 GB=8.4 GB
```

Espaço de log de archive

O Operations Center usa aproximadamente 8 GB de espaço de log de archive a cada 24 horas, para cada 1000 clientes. No exemplo de 6500 clientes no servidor do hub e nos servidores spoke, 56 GB de espaço de log de archive são usados por um período de 24 horas para o servidor do hub.

Para cada servidor spoke no exemplo, o espaço do log de archive que é usado por 24 horas é de aproximadamente 16 GB. Essas estimativas são baseadas no intervalo de coleta de status padrão de 5 minutos. Se você reduzir o intervalo de coleta de uma vez a cada 5 minutos para uma vez a

cada 3 minutos, os requisitos de espaço aumentarão. Os exemplos a seguir mostram o aumento aproximado no requisito de espaço de log com um intervalo de coleta de uma vez a cada 3 minutos:

- Servidor do hub: de 56 GB para aproximadamente 94 GB
- Cada servidor spoke: de 16 GB para aproximadamente 28 GB

Aumente o espaço de log de archive para que haja espaço suficiente disponível para suportar o Operations Center, sem afetar as operações do servidor existentes.

Requisitos de hardware para o segundo servidor

Se você estiver planejando configurar seus sites para que tudo no primeiro site seja replicado para o segundo site, os requisitos de hardware serão idênticos em ambos os sites. Se desejar replicar apenas um subconjunto de dados para seu segundo site, os requisitos de armazenamento e de rede podem ser reduzidos.

Requisitos de Software

A documentação para a solução de disco multisite IBM Spectrum Protect inclui tarefas de instalação e configuração para os sistemas operacionais a seguir. É necessário atender aos requisitos mínimos de software que são listados.

Para obter informações sobre os requisitos de software para os drivers de dispositivo lin_tape da IBM, consulte o .

Sistemas AIX

Tipo de software	Requisitos Mínimos de Software
Sistema Operacional	IBM AIX 7.1 Para obter mais informações sobre os requisitos do sistema operacional, consulte AIX: requisitos mínimos do sistema para sistemas AIX.
Utilitário Gunzip	O utilitário gunzip deve estar disponível em seu sistema antes de você instalar ou fazer upgrade do servidor IBM Spectrum Protect . Certifique-se de que o utilitário gunzip esteja instalado e o caminho para ele esteja configurado na variável de ambiente PATH.

Tipo de software	Requisitos Mínimos de Software
Tipo de sistema de arquivos	Sistemas de arquivos JFS2 Os sistemas AIX podem armazenar em cache uma grande quantidade de dados do sistema de arquivos, o que pode reduzir a memória necessária para os processos do servidor e do IBM Db2. Para evitar paginação com o servidor AIX, use a opção de montagem `rbrw` para o sistema de arquivos JFS2. Menos memória é usada para o cache do sistema de arquivos e mais está disponível para o IBM Spectrum Protect. Não use as opções de montagem do sistema de arquivos, Concurrent I/O (CIO) e Direct I/O (DIO), para sistemas de arquivos que contêm o banco de dados do IBM Spectrum Protect, logs ou volumes do conjunto de armazenamentos. Essas opções podem causar degradação de desempenho de muitas operações do servidor. O IBM Spectrum Protect e o Db2 ainda podem usar o DIO se isso for benéfico, mas o IBM Spectrum Protect não requererá as opções de montagem para aproveitar seletivamente essas técnicas.
Outro software	Korn Shell (ksh)

Sistemas Linux

Tipo de software	Requisitos Mínimos de Software
Sistema Operacional	Red Hat Enterprise Linux 7 (x86_64)
Bibliotecas	Bibliotecas GNU C, Versão 2.3.3-98.38 ou posterior, que estejam instaladas no sistema IBM Spectrum Protect. Red Hat Enterprise Linux Servers: • libaio • libstdc++.so.6 (os pacotes de 32 bits e de 64 bits são necessários) • numactl.x86_64
Tipo de sistema de arquivos	Sistemas de arquivos relacionados ao banco de dados de formato com ext3 ou ext4. Para sistemas de arquivos relacionados ao conjunto de armazenamentos, use XFS.
Outro software	Korn Shell (ksh)

Sistemas Windows

Tipo de software	Requisitos Mínimos de Software
Sistema Operacional	Microsoft Windows Server 2012 R2 (64 bits) ou Windows Server 2016
Tipo de sistema de arquivos	NTFS

Tipo de software	Requisitos Mínimos de Software
Outro software	O Windows 2012 R2 ou Windows 2016 com .NET Framework 3.5 está instalado e ativado. As políticas a seguir de Controle de Conta do Usuário devem ser desativadas: • Controle de Conta do Usuário: Modo de Aprovação do Administrador para contagem do Administrador Integrado • Controle de Conta do Usuário: Execute todos os administradores no Modo de Aprovação do Administrador

Tarefas relacionadas:

Configurando opções de rede do AIX

Capítulo 4. Planilhas de planejamento

Use as planilhas de planejamento para registrar valores que são usados para configurar o sistema e configurar o servidor do IBM Spectrum Protect. Use os valores padrão de melhor prática que estão listados nas planilhas.

Cada planilha ajuda-o a preparar-se para diferentes partes da configuração do sistema usando valores de melhor prática:

Pré-configuração do sistema do servidor
Use as planilhas de pré-configuração para planejar os sistemas de arquivos e diretórios criados ao configurar sistemas de arquivos para o IBM Spectrum Protect durante a configuração de sistema. Todos os diretórios que você criar para o servidor devem estar vazios.

Configuração do servidor
Use as planilhas de configuração quando configurar o servidor. Os valores padrão são sugeridos para a maioria dos itens, exceto onde indicado.

AIX

Tabela 2. Planilha para pré-configuração de um sistema do servidor AIX

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas
Endereço de porta TCP/IP para comunicações com o servidor	1500		Não aplicável	Certifique-se de que essa porta esteja disponível ao instalar e configurar o sistema operacional O número da porta pode ser um número no intervalo de 1024 a 32767.
Diretório da instância do servidor	`/home/tsminst1/tsminst1`		50 GB	Se você mudar o valor padrão do diretório de instância do servidor, modifique também o valor do proprietário da instância do Db2 no Tabela 3 na página 16.
Diretório para instalação de servidor	`/`		Espaço disponível que é necessário para o diretório: 5 GB	
Diretório para instalação de servidor	`/usr`		Espaço disponível que é necessário para o diretório: 5 GB	

Tabela 2. Planilha para pré-configuração de um sistema do servidor AIX (continuação)

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas
Diretório para instalação de servidor	`/var`		Espaço disponível que é necessário para o diretório: 5 GB	
Diretório para instalação de servidor	`/tmp`		Espaço disponível que é necessário para o diretório: 5 GB	
Diretório para instalação de servidor	`/opt`		Espaço disponível que é necessário para o diretório: 10 GB	
Diretório para o log ativo	`/tsminst1/TSMalog`		• Pequeno e médio: 140 GB • Grande: 300 GB	Ao criar o log ativo durante a configuração inicial do servidor, configure o tamanho como 128 GB.
Diretório para o log de archive	`/tsminst1/TSMarchlog`		• Pequeno: 1 TB • Médio: 2 TB • Grande: 4 TB	

Diretórios para o banco de dados	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 1 TB
			• Médio: Pelo menos 2 TB
			• Grande: Pelo menos 4 TB
				Crie um número mínimo de sistemas de arquivos para o banco de dados, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 4 sistemas de arquivos
				• Médio: Pelo menos 4 sistemas de arquivos
				• Grande: Pelo menos 8 sistemas de arquivos

Tabela 2. Planilha para pré-configuração de um sistema do servidor AIX (continuação)

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas

Diretórios para armazenamento	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 38 TB
			• Médio: Pelo menos 180 TB
			• Grande: Pelo menos 500 TB
				Crie um número mínimo de sistemas de arquivos para armazenamento, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 10 sistemas de arquivos
				• Médio: Pelo menos 20 sistemas de arquivos
				• Grande: Pelo menos 40 sistemas de arquivos

Diretórios para backup de banco de dados	`/tsminst1/TSMbkup00`
	`/tsminst1/TSMbkup01`
	`/tsminst1/TSMbkup02`
	`/tsminst1/TSMbkup03`
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 3 TB
			• Médio: Pelo menos 10 TB
			• Grande: Pelo menos 16 TB
				Crie um número mínimo de sistemas de arquivos para fazer backup do banco de dados, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 2 sistemas de arquivos
				• Médio: Pelo menos 4 sistemas de arquivos
				• Grande: pelo menos 4 sistemas de arquivos, mas de preferência 6
				
				O primeiro diretório de backup do banco de dados, que também é usado para o diretório de failover do log de archive, e uma segunda cópia do histórico do volume e dos arquivos de configuração de dispositivo.

Tabela 3. Planilha para configuração do IBM Spectrum Protect

Item	Valor padrão	Seu valor	Notas
Proprietário da instância do Db2	`tsminst1`		Se você mudou o valor padrão do diretório de instância do servidor no Tabela 2 na página 13, modifique também o valor para o proprietário da instância do Db2.
Senha do proprietário da instância do Db2	`passw0rd`		Selecione um valor para a senha do proprietário da instância diferente do padrão. Certifique-se de registrar esse valor em um local seguro.
Grupo primário para o proprietário da instância do Db2	`tsmsrvrs`		
Nome do Servidor	O valor padrão para o nome do servidor é o nome do host do sistema.		
Senha do servidor	`passw0rd`		Selecione um valor diferente do padrão para a senha do servidor. Certifique-se de registrar esse valor em um local seguro.
ID de administrador: ID do usuário para a instância do servidor	`admin`		
Senha de ID de administrador	`passw0rd`		Selecione um valor diferente do padrão para a senha do administrador. Certifique-se de registrar esse valor em um local seguro.

Tabela 3. Planilha para configuração do IBM Spectrum Protect (continuação)

Item	Valor padrão	Seu valor	Notas
Horário de início do planejamento	`22:00`		O horário de início de planejamento padrão inicia a fase de carga de trabalho do cliente, que são predominantemente as atividades de backup e archive do cliente. Durante a fase de carga de trabalho do cliente, os recursos do servidor suportam operações do cliente. Normalmente, essas operações são concluídas durante a janela de planejamento noturna. Os planejamentos para operações de manutenção do servidor são definidos para iniciar 10 horas após o início da janela de backup do cliente.

Linux

Tabela 4. Planilha para pré-configuração de um sistema do servidor Linux

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas
Endereço de porta TCP/IP para comunicações com o servidor	1500		Não aplicável	Certifique-se de que essa porta esteja disponível ao instalar e configurar o sistema operacional O número da porta pode ser um número no intervalo de 1024 a 32767.
Diretório da instância do servidor	`/home/tsminst1/tsminst1`		25 GB	Se você mudar o valor padrão do diretório de instância do servidor, modifique também o valor do proprietário da instância do Db2 no Tabela 5 na página 19.
Diretório para o log ativo	`/tsminst1/TSMalog`		• Pequeno e médio: 140 GB • Grande: 300 GB	

Tabela 4. Planilha para pré-configuração de um sistema do servidor Linux (continuação)

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas
Diretório para o log de archive	`/tsminst1/TSMarchlog`		• Pequeno: 1 TB • Médio: 2 TB • Grande: 4 TB	

Diretórios para o banco de dados	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 1 TB
			• Médio: Pelo menos 2 TB
			• Grande: Pelo menos 4 TB
				Crie um número mínimo de sistemas de arquivos para o banco de dados, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 4 sistemas de arquivos
				• Médio: Pelo menos 4 sistemas de arquivos
				• Grande: Pelo menos 8 sistemas de arquivos

Diretórios para armazenamento	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 38 TB
			• Médio: Pelo menos 180 TB
			• Grande: Pelo menos 500 TB
				Crie um número mínimo de sistemas de arquivos para armazenamento, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 10 sistemas de arquivos
				• Médio: Pelo menos 20 sistemas de arquivos
				• Grande: Pelo menos 40 sistemas de arquivos

Tabela 4. Planilha para pré-configuração de um sistema do servidor Linux (continuação)

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas

Diretórios para backup de banco de dados	`/tsminst1/TSMbkup00`
	`/tsminst1/TSMbkup01`
	`/tsminst1/TSMbkup02`
	`/tsminst1/TSMbkup03`
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 3 TB
			• Médio: Pelo menos 10 TB
			• Grande: Pelo menos 16 TB
				Crie um número mínimo de sistemas de arquivos para fazer backup do banco de dados, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 2 sistemas de arquivos
				• Médio: Pelo menos 4 sistemas de arquivos
				• Grande: pelo menos 4 sistemas de arquivos, mas de preferência 6
				O primeiro diretório de backup do banco de dados, que também é usado para o diretório de failover do log de archive, e uma segunda cópia do histórico do volume e dos arquivos de configuração de dispositivo.

Tabela 5. Planilha para configuração do IBM Spectrum Protect

Item	Valor padrão	Seu valor	Notas
Proprietário da instância do Db2	`tsminst1`		Se você mudou o valor padrão do diretório de instância do servidor no Tabela 4 na página 17, modifique também o valor para o proprietário da instância do Db2.
Senha do proprietário da instância do Db2	`passw0rd`		Selecione um valor para a senha do proprietário da instância diferente do padrão. Certifique-se de registrar esse valor em um local seguro.
Grupo primário para o proprietário da instância do Db2	`tsmsrvrs`		
Nome do Servidor	O valor padrão para o nome do servidor é o nome do host do sistema.		

Tabela 5. Planilha para configuração do IBM Spectrum Protect (continuação)

Item	Valor padrão	Seu valor	Notas
Senha do servidor	`passw0rd`		Selecione um valor diferente do padrão para a senha do servidor. Certifique-se de registrar esse valor em um local seguro.
ID de administrador: ID do usuário para a instância do servidor	`admin`		
Senha de ID de administrador	`passw0rd`		Selecione um valor diferente do padrão para a senha do administrador. Certifique-se de registrar esse valor em um local seguro.
Horário de início do planejamento	`22:00`		O horário de início de planejamento padrão inicia a fase de carga de trabalho do cliente, que são predominantemente as atividades de backup e archive do cliente. Durante a fase de carga de trabalho do cliente, os recursos do servidor suportam operações do cliente. Normalmente, essas operações são concluídas durante a janela de planejamento noturna. Os planejamentos para operações de manutenção do servidor são definidos para iniciar 10 horas após o início da janela de backup do cliente.

Windows

Como muitos volumes são criados para o servidor, configure o servidor usando o recurso do Windows de mapeamento de volumes de disco para diretórios em vez de letras de unidade.

Por exemplo, `C:\tsminst1\TSMdbpsace00` é um ponto de montagem para um volume com seu próprio espaço. O volume é mapeado para um diretório na unidade C:, mas não ocupa espaço da unidade C:. A exceção é o diretório de instância do servidor, `C:\tsminst1`, que pode ser um ponto de montagem ou um diretório regular.

Tabela 6. Planilha para pré-configuração de um sistema do servidor Windows

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas
Endereço de porta TCP/IP para comunicações com o servidor	1500		Não aplicável	Certifique-se de que essa porta esteja disponível ao instalar e configurar o sistema operacional O número da porta pode ser um número no intervalo de 1024 a 32767.
Diretório da instância do servidor	`C:\tsminst1`		25 GB	Se você mudar o valor padrão do diretório de instância do servidor, modifique também o valor do proprietário da instância do Db2 no Tabela 7 na página 23.
Diretório para o log ativo	`C:\tsminst1\TSMalog`		• Pequeno e médio: 140 GB • Grande: 300 GB	
Diretório para o log de archive	`C:\tsminst1\TSMarchlog`		• Pequeno: 1 TB • Médio: 2 TB • Grande: 4 TB	

Diretórios para o banco de dados	`C:\tsminst1\TSMdbspace00`
	`C:\tsminst1\TSMdbspace01`
	`C:\tsminst1\TSMdbspace02`
	`C:\tsminst1\TSMdbspace03`
	...
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 1 TB
			• Médio: Pelo menos 2 TB
			• Grande: Pelo menos 4 TB
				Crie um número mínimo de sistemas de arquivos para o banco de dados, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 4 sistemas de arquivos
				• Médio: Pelo menos 4 sistemas de arquivos
				• Grande: Pelo menos 8 sistemas de arquivos

Tabela 6. Planilha para pré-configuração de um sistema do servidor Windows (continuação)

Item	Valor padrão	Seu valor	Tamanho mínimo do diretório	Notas

Diretórios para armazenamento	`C:\tsminst1\TSMfile00`
	`C:\tsminst1\TSMfile01`
	`C:\tsminst1\TSMfile02`
	`C:\tsminst1\TSMfile03`
	...
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 38 TB
			• Médio: Pelo menos 180 TB
			• Grande: Pelo menos 500 TB
				Crie um número mínimo de sistemas de arquivos para armazenamento, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 10 sistemas de arquivos
				• Médio: Pelo menos 20 sistemas de arquivos
				• Grande: Pelo menos 40 sistemas de arquivos

Diretórios para backup de banco de dados	`C:\tsminst1\TSMbkup00`
	`C:\tsminst1\TSMbkup01`
	`C:\tsminst1\TSMbkup02`
	`C:\tsminst1\TSMbkup03`
			Espaço total mínimo para todos os diretórios:
			• Pequeno: Pelo menos 3 TB
			• Médio: Pelo menos 10 TB
			• Grande: Pelo menos 16 TB
				Crie um número mínimo de sistemas de arquivos para fazer backup do banco de dados, dependendo do tamanho de seu sistema:
				• Pequeno: Pelo menos 2 sistemas de arquivos
				• Médio: Pelo menos 4 sistemas de arquivos
				• Grande: pelo menos 4 sistemas de arquivos, mas de preferência 6
				
				O primeiro diretório de backup do banco de dados, que também é usado para o diretório de failover do log de archive, e uma segunda cópia do histórico do volume e dos arquivos de configuração de dispositivo.

Tabela 7. Planilha para configuração do IBM Spectrum Protect

Item	Valor padrão	Seu valor	Notas
Proprietário da instância do Db2	`tsminst1`		Se você mudou o valor padrão do diretório de instância do servidor no Tabela 6 na página 21, modifique também o valor para o proprietário da instância do Db2.
Senha do proprietário da instância do Db2	`pAssW0rd`		Selecione um valor para a senha do proprietário da instância diferente do padrão. Certifique-se de registrar esse valor em um local seguro.
Nome do Servidor	O valor padrão para o nome do servidor é o nome do host do sistema.		
Senha do servidor	`passw0rd`		Selecione um valor diferente do padrão para a senha do servidor. Certifique-se de registrar esse valor em um local seguro.
ID de administrador: ID do usuário para a instância do servidor	`admin`		
Senha de ID de administrador	`passw0rd`		Selecione um valor diferente do padrão para a senha do administrador. Certifique-se de registrar esse valor em um local seguro.
Horário de início do planejamento	`22:00`		O horário de início de planejamento padrão inicia a fase de carga de trabalho do cliente, que são predominantemente as atividades de backup e archive do cliente. Durante a fase de carga de trabalho do cliente, os recursos do servidor suportam operações do cliente. Normalmente, essas operações são concluídas durante a janela de planejamento noturna. Os planejamentos para operações de manutenção do servidor são definidos para iniciar 10 horas após o início da janela de backup do cliente.

Capítulo 5. Planejando o armazenamento

Escolha a tecnologia de armazenamento mais eficaz para componentes do IBM Spectrum Protect para assegurar o desempenho e operações eficientes do servidor.

Os dispositivos de hardware de armazenamento possuem diferentes características de capacidade e desempenho, que determinam como podem ser usadas de forma eficiente com o IBM Spectrum Protect. Para obter orientação geral sobre a seleção de hardware de armazenamento apropriado e configurar sua solução, revise as diretrizes a seguir.

Banco de dados e log ativo

- Use um disco rápido para o banco de dados e log ativo do IBM Spectrum Protect, por exemplo, com as seguintes características:
  - Disco de 15k rpm de alto desempenho, com interface Fibre Channel ou serial-attached SCSI (SAS)
  - Disco de estado sólido (SSD)
- Isole o log ativo do banco de dados, a menos que você use SSD ou hardware flash
- Ao criar matrizes para o banco de dados, use o nível 5 do RAID

Conjunto de armazenamentos

- É possível usar discos menos dispendiosos e mais lentos para o conjunto de armazenamentos
- O conjunto de armazenamentos pode compartilhar discos para o log de archive e armazenamento de backup de banco de dados
- Use o nível 6 do RAID para matrizes do conjunto de armazenamentos para incluir proteção contra falhas de unidades duplas ao usar tipos de discos grandes

Referências relacionadas:

Requisitos do sistema de armazenamento e como reduzir o risco de distorção de dados

Planejando as matrizes de armazenamento

Prepare a configuração de armazenamento em disco planejando matrizes e volumes RAID de acordo com o tamanho do sistema IBM Spectrum Protect.

Você projeta as matrizes de armazenamento com características de tamanho e de desempenho que sejam adequadas para um dos componentes de armazenamento do servidor do IBM Spectrum Protect, como o banco de dados do servidor ou um conjunto de armazenamentos. A atividade de planejamento de armazenamento deve considerar o tipo de unidade, o nível do RAID, o número de unidades, o número de unidades sobressalentes, etc. Nas configurações de solução, os grupos de armazenamentos contêm matrizes RAID de armazenamento interno e consistem em vários discos físicos que são apresentados como volumes lógicos no sistema. Ao configurar o sistema de armazenamento em disco, você cria grupos de armazenamentos, ou conjuntos de armazenamentos de dados e, em seguida, cria matrizes de armazenamento nos grupos.

Você cria volumes, ou LUNs, a partir dos grupos de armazenamentos. O grupo de armazenamentos define quais discos fornecem o armazenamento que forma o volume. Ao criar volumes, torne-os totalmente alocados. Os tipos de discos mais rápidos são usados para conter os volumes do banco de dados e volumes de log ativo. Os tipos de discos mais lentos podem ser usados para os volumes do conjunto de armazenamentos, log de archive e volumes de backup de banco de dados. Se você usar um conjunto de armazenamentos em disco menor para estagiar dados, poderá ser necessário usar discos mais rápidos para gerenciar o desempenho da carga de trabalho diária para ingerir e migrar dados.

A Tabela 8 e a Tabela 9 descrevem os requisitos de layout para grupos de armazenamentos e configuração de volume.

Tabela 8. Componentes de configuração do grupo de armazenamentos

Componente	**Detalhes**
Requisito de armazenamento do servidor	Como o armazenamento é usado pelo servidor.
Tipo de disco	Tamanho e velocidade para o tipo de disco que é usado para o requisito de armazenamento.
Quantidade de disco	Número de cada tipo de disco que é necessário para o requisito de armazenamento.
Capacidade de hot spare	Número de discos que são reservados como sobressalentes para assumir o controle se ocorrerem falhas de disco.
Nível do RAID	Nível de matriz RAID que é usado para armazenamento lógico. O nível do RAID define o tipo de redundância que é fornecido pela matriz, por exemplo, 5 ou 6.
Quantidade de matrizes RAID	Número de matrizes RAID a serem criadas.
DDMs por matriz RAID	Quantos módulos da unidade de disco (DDMs) devem ser usados em cada uma das matrizes RAID.
Tamanho utilizável por matriz RAID	Tamanho que está disponível para armazenamento de dados em cada matriz RAID após contabilizar o espaço perdido devido à redundância.
Tamanho utilizável total	Tamanho total que está disponível para armazenamento de dados nas matrizes RAID: `Quantidade x tamanho utilizável`
Nomes sugeridos de grupos de armazenamentos e de matrizes	Nome preferencial a ser usado para MDisks e grupos de MDisk.
Uso	Componente do servidor que usa parte do disco físico.

Tabela 9. Componentes da configuração de volume

Componente	**Detalhes**
Requisito de armazenamento do servidor	Requisito para o qual o disco físico é usado.
Nome do volume	Nome exclusivo que é dado a um volume específico.
Grupo de armazenamentos	Nome do grupo de armazenamento do qual o espaço é obtido para criar o volume.

Tabela 9. Componentes da configuração de volume (continuação)

Componente	Detalhes
Tamanho	Tamanho de cada volume.
Ponto de montagem do servidor desejado	Diretório no sistema do servidor no qual o volume é montado.
Quantidade	Número de volumes a serem criados para um requisito específico. Use o mesmo padrão de nomenclatura para cada volume que é criado para o mesmo requisito.
Uso	Componente do servidor que usa parte do disco físico.

Exemplos

Exemplos de configuração para grupos de armazenamentos e volumes estão disponíveis no link a seguir: Exemplos de planilhas para o planejamento de matrizes de armazenamento. Os exemplos mostram como planejar o armazenamento para tamanhos de servidores diferentes. Nas configurações de exemplo, há um mapeamento um-para-um entre discos e grupos de armazenamentos. É possível fazer download dos exemplos e editar as planilhas para planejar a configuração de armazenamento para seu servidor.

Capítulo 6. Planejando a segurança

Planeje proteger a segurança de sistemas na solução do IBM Spectrum Protect com controles de acesso e autenticação, e considere criptografar a transmissão de dados e de senha.

Para obter diretrizes sobre como proteger seu ambiente de armazenamento contra ataques de ransomware e como recuperar o seu ambiente de armazenamento se um ataque ocorrer, consulte Proteger o ambiente de armazenamento contra ransomware.

Planejando funções de administrador

Defina os níveis de autoridade que você deseja designar a administradores que têm acesso à solução do IBM Spectrum Protect.

É possível designar um dos seguintes níveis de autoridade a administradores:

Sistema
Administradores com autoridade do sistema têm o nível de autoridade mais alto. Os administradores com este nível de autoridade podem concluir qualquer tarefa. Eles podem gerenciar todos os domínios de política e conjuntos de armazenamentos e conceder autoridade a outros administradores.

Política
Os administradores que possuem autoridade de política podem gerenciar todas as tarefas relacionadas ao gerenciamento de política. Esse privilégio pode ser irrestrito ou pode ser restrito a domínios de política específicos.

Armazenamento
Os administradores que possuírem autoridade de armazenamento podem alocar e controlar recursos de armazenamento para o servidor.

Operador
Os administradores que possuírem autoridade de operador podem controlar a operação imediata do servidor e a disponibilidade de mídia de armazenamento, como bibliotecas e unidades de fitas.

Os cenários na Tabela 10 fornecem exemplos sobre por que talvez você queira designar níveis variados de autoridade para que os administradores possam executar tarefas:

Tabela 10. Cenários para funções de administrador

Cenário	Tipo de ID de administrador para configuração
Um administrador em uma empresa pequena gerencia o servidor e é responsável por todas as atividades do servidor.	• Autoridade do sistema: 1 ID de administrador
Um administrador para vários servidores também gerencia o sistema geral. Vários outros administradores gerenciam seus próprios conjuntos de armazenamentos.	• Autoridade do sistema em todos os servidores: 1 ID de administrador para o administrador do sistema geral • Autoridade de armazenamento para conjuntos de armazenamentos designados: 1 ID de administrador para cada um dos outros administradores

Tabela 10. Cenários para funções de administrador (continuação)

Cenário	Tipo de ID de administrador para configuração
Um administrador gerencia 2 servidores. Outra pessoa ajuda com as tarefas de administração. Dois assistentes são responsáveis por ajudar a assegurar que seja feito backup dos sistemas importantes. Cada assistente é responsável por monitorar os backups planejados em um dos servidores do IBM Spectrum Protect.	• Autoridade do sistema em ambos os servidores: 2 IDs de administrador • Autoridade de operador: 2 IDs de administrador para os assistentes com acesso ao servidor pelo qual cada pessoa é responsável

Planejando comunicações seguras

Planejar-se para proteger as comunicações entre os componentes da solução IBM Spectrum Protect.

Determine o nível de proteção que é necessário para seus dados, com base nos regulamentos e necessidades de negócios nos quais sua empresa opera.

Se sua empresa requer um alto nível de segurança para senhas e transmissão de dados, planeje implementar a comunicação segura com os protocolos Segurança da Camada de Transporte (TLS) ou Secure Sockets Layer (SSL).

O TLS e o SSL fornecem comunicações seguras entre o servidor e o cliente, mas podem afetar o desempenho do sistema. Para melhorar o desempenho do sistema, use TLS para autenticação sem criptografar dados do objeto. Para especificar se o servidor usa TLS 1.2 para a sessão inteira ou somente para autenticação, consulte a opção do cliente SSL para comunicação cliente-para-servidor e o parâmetro **UPDATE SERVER=SSL** para comunicação servidor-para-servidor. Iniciando na V8.1.2, o TLS é usado para autenticação, por padrão. Se você decidir usar TLS para criptografar sessões inteiras, use o protocolo somente para sessões em que ele é necessário e inclua recursos do processador no servidor para gerenciar o aumento no tráfego de rede. Você também pode tentar outras opções. Por exemplo, alguns dispositivos de rede, como roteadores e comutadores, fornecem a função TLS ou SSL.

É possível usar TLS e SSL para proteger alguns ou todos os diferentes caminhos de comunicação possíveis, por exemplo:

- Operations Center: navegador para hub; hub para spoke
- Cliente para servidor
- Servidor para servidor: replicação de nó

Tarefas relacionadas:

Protegendo Comunicações

Planejando o armazenamento de dados criptografados

Determine se sua empresa requer que os dados armazenados sejam criptografados e escolha a opção mais adequada às suas necessidades.

Se sua empresa requer que os dados nos conjuntos de armazenamentos sejam criptografados, há a opção de usar a criptografia do IBM Spectrum Protect ou um dispositivo externo, como fita para criptografia.

Se escolher o IBM Spectrum Protect para criptografar os dados, recursos de computação extras serão necessários no cliente que podem afetar o desempenho dos processos de backup e de restauração.

Informações relacionadas:

nota técnica 1963635

Planejando acesso ao firewall

Determine os firewalls que estão configurados e as portas que devem ser abertas para o funcionamento da solução do IBM Spectrum Protect.

Tabela 11 descreve as portas que são usadas pelo servidor, cliente e Operations Center.

Tabela 11. Portas que são usadas pelo servidor, pelo cliente e o Operations Center

Item	Padrão	Direção	descrição
Porta base (**TCPPORT**)	1500	Saída/ entrada	Cada instância do servidor requer uma porta exclusiva. É possível especificar um número de porta alternativo em vez de usar o padrão. A opção **TCPPORT** atende a sessões ativadas para TCP/IP e SSL do cliente. Para o tráfego do cliente administrativo, é possível usar as opções **TCPADMINPORT** e **ADMINONCLIENTPORT** para configurar os valores de porta.
Porta somente SSL (**SSLTCPPORT**)	Sem padrão	Saída/ entrada	Essa porta será usada se você desejar restringir a comunicação na porta somente a sessões ativadas para SSL. Para suportar as comunicações de SSL e que não são de SSL, use as opções **TCPPORT** ou **TCPADMINPORT**.
SMB	45	Entrada/ saída	Essa porta é usada por assistentes de configuração que se comunicam usando protocolos nativos com vários hosts.
SSH	22	Entrada/ saída	Essa porta é usada por assistentes de configuração que se comunicam usando protocolos nativos com vários hosts.
SMTP	25	Saída	Esta porta é usada para enviar alertas de e-mail do servidor.

Tabela 11. Portas que são usadas pelo servidor, pelo cliente e o Operations Center (continuação)

Item	Padrão	Direção	descrição
NDMP	Sem padrão	Entrada/ saída	O servidor deve ser capaz de abrir uma conexão da porta de controle NDMP de saída para o dispositivo NAS. A porta de controle de saída é o Endereço de baixo nível na definição do movedor de dados para o dispositivo NAS. Durante uma restauração de arquivador-para-servidor NDMP, o servidor deve ser capaz de abrir uma conexão de dados NDMP de saída para o dispositivo NAS. A porta de conexão de dados que é usada durante uma restauração pode ser configurada no dispositivo NAS. Durante backups de arquivador-para-servidor NDMP, o dispositivo NAS deve ser capaz de abrir conexões de dados de saída para o servidor e o servidor deve ser capaz de aceitar conexões de dados NDMP de entrada. É possível usar a opção do servidor **NDMPPORTRANGE** para restringir o conjunto de portas disponíveis para uso como conexões de dados NDMP. É possível configurar um firewall para conexões com essas portas.
Replicação	Sem padrão	Saída/ entrada	A porta e protocolo para a porta de saída para replicação são configurados pelo comando **DEFINE SERVER** que é usado para configurar a replicação. As portas de entrada para replicação são as portas TCP e portas SSL que o servidor de origem nomeia nos comandos **DEFINE SERVER**.
Porta de planejamento de cliente	Porta do cliente: 1501	Saída	O cliente atende na porta nomeada e comunica o número da porta ao servidor. O servidor entra em contato com o cliente se o planejamento solicitado pelo servidor for usado. É possível especificar um número de porta alternativo no arquivo de opções do cliente.
Sessões de longa execução	Configuração de **KEEPALIVE**: YES	Saída	Quando a opção **KEEPALIVE** estiver ativada, os pacotes keep-alive serão enviados durante sessões do cliente/servidor para evitar que o software de firewall feche conexões de longa execução e inativas.
Operations Center	HTTPS: 11090	Entrada	Essas portas são usadas para o navegador da web do Operations Center. É possível especificar um número de porta alternativo.

Tabela 11. Portas que são usadas pelo servidor, pelo cliente e o Operations Center (continuação)

Item	Padrão	Direção	descrição
Porta de serviço de gerencia mento de cliente	Porta do cliente: 9028	Entrada	A porta de serviço de gerenciamento de cliente deve ser acessível a partir do Operations Center. Assegure-se de que os firewalls não possam impedir conexões. O serviço de gerenciamento de cliente usa a porta TCP do servidor para o nó cliente para autenticação usando uma sessão administrativa.

Parte 2. Implementação de disco multisite de uma solução de proteção de dados

A solução de disco multisite é configurada em dois sites e usa deduplicação e replicação de dados.

Roteiro de implementação

As etapas a seguir são necessárias para configurar um ambiente de disco multisite.

1. Configurar o sistema.
   a. Configurar o hardware de armazenamento e configurar matrizes de armazenamento para o tamanho de seu ambiente.
   b. Instalar o sistema operacional do servidor.
   c. Configurar E/S de caminhos múltiplos.
   d. Criar o ID do usuário para a instância do servidor.
   e. Preparar sistemas de arquivos para o IBM Spectrum Protect.
2. Instalar o servidor e o Operations Center.
3. Configurar o servidor e o Operations Center.
   a. Concluir a configuração inicial do servidor.
   b. Configurar opções do servidor.
   c. Configurar o Secure Sockets Layer para o servidor e o cliente.
   d. Configurar o Operations Center.
   e. Registrar sua licença do IBM Spectrum Protect.
   f. Configurar a deduplicação de dados.
   g. Definir regras de retenção de dados para seus negócios.
   h. Definir planejamentos de manutenção do servidor.
   i. Definir planejamentos de cliente.
4. Instalar e configurar clientes.
   a. Registrar e designar clientes a planejamentos.

      Dica: Evite conflitos no gerenciamento de IDs administrativos e de conjuntos de opções do cliente, identificando os IDs e os conjuntos de opções que serão replicados para o servidor de destino e os IDs e os conjuntos de opções que serão gerenciados em uma configuração corporativa. Não será possível definir um ID do usuário administrativo para um nó registrado se um ID administrativo existir para o mesmo nó.
   b. Instalar e verificar o serviço de gerenciamento de clientes.
   c. Configurar o Operations Center para usar o serviço de gerenciamento de clientes.
5. Configurar o segundo servidor.
   a. Configurar a comunicação de SSL entre o servidor do hub e o spoke.
   b. Incluir o segundo servidor como um spoke.
   c. Ativar replicação.
6. Concluir a implementação.

Capítulo 7. Configurando o sistema

Para configurar o sistema, primeiro é necessário configurar o hardware de armazenamento em disco e o sistema do servidor para o IBM Spectrum Protect.

Configurando o hardware de armazenamento

Para configurar o hardware de armazenamento, revise a orientação geral para sistemas de disco e o IBM Spectrum Protect.

Procedimento

1. Forneça uma conexão entre o servidor e os dispositivos de armazenamento seguindo estas diretrizes:
   - Use um comutador ou conexão direta para conexões Fibre Channel.
   - Considere o número de portas conectadas e considere a quantia de largura da banda que é necessária.
   - Considere o número de portas no servidor e o número de portas do host no sistema de disco que estão conectadas.
2. Verifique se os drivers de dispositivo e o firmware para o sistema do servidor, adaptadores e o sistema operacional são atuais e nos níveis recomendados.
3. Configure as matrizes de armazenamento. Assegure-se de ter planejado adequadamente para garantir o desempenho ideal. Consulte Capítulo 5, “Planejando o armazenamento”, na página 25 para obter informações adicionais.
4. Assegure-se de que o sistema do servidor tenha acesso a volumes de disco criados. Execute as etapas a seguir:
   a. Se o sistema estiver conectado a um comutador Fibre Channel, particione o servidor para ver os discos.
   b. Mapeie todos os volumes para informar o sistema de disco de que esse servidor específico tem permissão de ver cada disco.

Tarefas relacionadas:

Configurando o armazenamento

Instalando o sistema operacional do servidor

Instale o sistema operacional no sistema do servidor e certifique-se de que os requisitos do servidor do IBM Spectrum Protect sejam atendidos. Ajuste as configurações do sistema operacional, conforme instruções.

Instalando em sistemas AIX

Conclua as etapas a seguir para instalar o AIX no sistema do servidor.

Procedimento

1. Instale o AIX Versão 7.1, TL4, SP2 ou mais recente de acordo com as instruções do fabricante.
2. Defina as configurações do TCP/IP de acordo com as instruções de instalação do sistema operacional.
3. Abra o arquivo `/etc/hosts` e conclua as seguintes ações:
   - Atualize o arquivo para incluir o endereço IP e o nome do host para o servidor. Por exemplo:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```
   - Verifique se o arquivo contém uma entrada para localhost com um endereço de 127.0.0.1. Por exemplo:

     ```
     127.0.0.1  localhost
     ```
4. Ative as portas de conclusão de E/S do AIX emitindo o seguinte comando:

   ```
   chdev -l iocp0 -P
   ```

   O desempenho do servidor pode ser afetado pela definição de fuso horário de Olson.
5. Para otimizar o desempenho, mude o formato de fuso horário do seu sistema de Olson para POSIX. Use o seguinte formato de comando para atualizar a configuração de fuso horário:

   ```
   chtz=local_timezone,date/time,date/time
   ```

   Por exemplo, se você morou em Tucson, Arizona, onde a Hora Padrão das Montanhas é usada, emita o seguinte comando para mudar para o formato POSIX:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```
6. Inclua uma entrada no `.profile` do usuário da instância de forma que o ambiente a seguir seja configurado:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

   Dica: Se o usuário da instância não estiver disponível, conclua esta etapa mais tarde, quando o usuário da instância se tornar disponível.
7. Configure o sistema para criar arquivos principais de aplicativo completos. Emita o seguinte comando:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```
8. Para comunicações com o servidor e oOperations Center, certifique-se de que as portas a seguir estejam abertas em quaisquer firewalls existentes:
   - Para comunicações com o servidor, abra a porta 1500.
   - Para comunicações seguras com o Operations Center, abra a porta 11090 no servidor do hub.

   Se você não estiver usando os valores de porta padrão, certifique-se de que as portas que estiverem sendo usadas estejam abertas.
9. Ative aprimoramentos de alto desempenho TCP. Emita o seguinte comando:

   ```
   no -p -o rfc1323=1
   ```
10. Para um rendimento e confiabilidade ideais, una quatro portas Ethernet de 10 Gb. Use o System Management Interface Tool (SMIT) para ligar as portas usando Etherchannel. As configurações a seguir foram usadas durante o teste:

```
mode            8023ad
auto_recovery   yes             Ativar recuperação automática após failover
backup_adapter  NONE            Adaptador utilizado quando o canal inteiro falha
hash_mode       src_dst_port    Determina como o adaptador de saída é escolhido
interval        long            Determina o valor do intervalo para IEEE
                                modo 802.3ad
mode            8023ad          Modo de operação EtherChannel
netaddr         0               Endereço para executar ping
noloss_failover yes             Ativar failover sem perdas após ping
                                falha
num_retries     3               Vezes para tentar executar ping novamente
                                antes de falhar
retry_time      1               Tempo de espera (em segundos) entre pings
use_alt_addr    no              Ativar Endereço de EtherChannel Alternativo
use_jumbo_frame no              Ativar Quadros Gigantes de Gigabit Ethernet
```

11. Verifique se os limites de recurso do processo do usuário, também conhecidos como *ulimits*, estão configurados de acordo com as diretrizes em Tabela 12. Se os valores de ulimit não estiverem configurados corretamente, pode haver instabilidade do servidor ou uma falha do servidor ao responder.

Tabela 12. Valores de limites do usuário (ulimit)

Tipo de limite do usuário	**Configuração**	**Valor**	**Comando para consultar valor**
Tamanho máximo dos arquivos principais criados	`core`	Sem limites	`ulimit -Hc`
Tamanho máximo de um segmento de dados para um processo	`dados`	Sem limites	`ulimit -Hd`
Tamanho máximo do arquivo	`fsize`	Sem limites	`ulimit -Hf`
Número máximo de arquivos abertos	`nofile`	65536	`ulimit -Hn`
Quantidade máxima de tempo do processador em segundos	`cpu`	Sem limites	`ulimit -Ht`
Número máximo de processos do usuário	`nproc`	16384	`ulimit -Hu`

Se precisar modificar quaisquer valores de limite do usuário, siga as instruções na documentação de seu sistema operacional.

Instalando em sistemas Linux

Conclua as etapas a seguir para instalar o Linux x86_64 no sistema do servidor.

Antes de Iniciar

O sistema operacional será instalado nos discos rígidos internos. Configure os discos rígidos internos usando uma matriz de hardware RAID 1. Por exemplo, se estiver configurando um sistema pequeno, os dois discos internos de 300 GB serão espelhados no RAID 1 para que um único disco de 300 GB apareça disponível para o instalador do sistema operacional.

Procedimento

1. Instale o Red Hat Enterprise Linux Versão 7.1 ou mais recente, de acordo com as instruções do fabricante. Obtenha um DVD inicializável que contenha o Red Hat Enterprise Linux Versão 7.1 e inicie seu sistema a partir desse DVD. Consulte a seguinte orientação para obter opções de instalação. Se um item não for mencionado na lista a seguir, deixe a seleção padrão.
   a. Depois de iniciar o DVD, escolha **Instalar ou fazer upgrade de um sistema existente** no menu.
   b. Na tela Bem-vindo, selecione **Testar essa mídia & instalar o Red Hat Enterprise Linux 7.1**.
   c. Selecione seu idioma e preferências do teclado.
   d. Selecione sua localização para configurar o fuso horário correto.
   e. Selecione **Seleção de software** e, em seguida, na próxima tela, selecione **Servidor com a GUI**.
   f. Na página de resumo de instalação, clique em **Destino de instalação** e verifique os itens a seguir:
      - O disco local de 300 GB está selecionado como o destino de instalação.
      - Em Outras opções de armazenamento, `Configurar particionamento automaticamente` está selecionado.

      Clique em **Pronto**.
   g. Clique em **Iniciar instalação**. Após o início da instalação, configure a senha root para a conta do usuário root.

   Após a instalação ser concluída, reinicie o sistema e efetue login como o usuário raiz. Emita o comando **df** para verificar seu particionamento básico. Por exemplo, em um sistema de teste, o particionamento inicial produziu o resultado a seguir:

```
[root@tvapp02]# df –h
Filesystem                      Size  Used  Avail  Use%  Mounted on
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G   1% /dev/shm
tmpfs                   32G  8.8M   32G   1% /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Defina as configurações do TCP/IP de acordo com as instruções de instalação do sistema operacional.

   Para um rendimento e confiabilidade ideais, considere ligar várias portas de rede. Isso pode ser feito criando uma conexão de rede Link Aggregation Control Protocol (LACP), que agrega várias portas subordinadas em uma única conexão lógica. O método preferencial é usar um modo de ligação de 802.3ad, uma configuração de **miimon** de 100 e uma configuração de **xmit_hash_policy** de layer3+4.

   Restrição: Para usar uma conexão de rede LACP, deve-se ter uma comutação de rede que suporte LACP.

   Para obter instruções adicionais sobre configurar conexões de rede ligadas ao Red Hat Enterprise Linux Versão 7, consulte Criar uma interface de ligação de canal.

3. Abra o arquivo `/etc/hosts` e conclua as seguintes ações:
   - Atualize o arquivo para incluir o endereço IP e o nome do host para o servidor. Por exemplo:

```
192.0.2.7  server.yourdomain.com  server
```

- Verifique se o arquivo contém uma entrada para localhost com um endereço de 127.0.0.1. Por exemplo:

```
127.0.0.1  localhost
```

4. Instale os componentes que são necessários para a instalação do servidor. Conclua as etapas a seguir para criar um repositório Yellowdog Updater Modified (YUM) e instalar os pacotes obrigatórios.
   a. Monte o DVD de instalação do Red Hat Enterprise Linux em um diretório do sistema. Por exemplo, para montá-lo no diretório `/mnt`, emita o seguinte comando:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b. Verifique se o DVD foi montado emitindo o comando **mount**. Você deve ver uma saída semelhante ao seguinte exemplo:

      ```
      /dev/sr0 on /mnt type iso9660
      ```

   c. Altere para o diretório do repositório YUM emitindo o seguinte comando:

      ```
      cd /etc/yum/repos.d
      ```

      Se o diretório `repos.d` não existir, crie-o.

   d. Liste o conteúdo do diretório:

      ```
      ls rhel-source.repo
      ```

   e. Renomeie o arquivo repo original emitindo o comando **mv**. Por exemplo:

      ```
      mv rhel-source.repo rhel-source.repo.orig
      ```

   f. Crie um novo arquivo repo usando um editor de texto. Por exemplo, para usar o editor de vi, emita o seguinte comando:

      ```
      vi rhel71_dvd.repo
      ```

   g. Inclua as seguintes linhas no novo arquivo repo. O parâmetro **baseurl** especifica o ponto de montagem de seu diretório:

      ```
      [rhel71_dvd]
      name=DVD Redhat Enterprise Linux 7.1
      baseurl=file:///mnt
      enabled=1
      gpgcheck=0
      ```

   h. Instale o pacote obrigatório `ksh.x86_64`, emitindo o comando **yum**. Por exemplo:

      ```
      yum install ksh.x86_64
      ```

      Exceção: Não é necessário instalar as bibliotecas `compat-libstdc++-33-3.2.3-69.el6.i686` e `libstdc++.i686` para o Red Hat Enterprise Linux Versão 7.1.

5. Quando a instalação de software estiver concluída, será possível restaurar os valores originais do repositório YUM concluindo as etapas a seguir:
   a. Desmonte o DVD de instalação do Red Hat Enterprise Linux emitindo o seguinte comando:

      ```
      unmount /mnt
      ```

   b. Altere para o diretório do repositório YUM emitindo o seguinte comando:

      ```
      cd /etc/yum/repos.d
      ```

   c. Renomeie o arquivo repo criado:

      ```
      mv rhel71_dvd.repo rhel71_dvd.repo.orig
      ```

   d. Renomeie o arquivo original para o nome original:

      ```
      mv rhel-source.repo.orig rhel-source.repo
      ```

6. Determine se as mudanças do parâmetro do kernel são necessárias. Execute as etapas a seguir:
   a. Use o comando **sysctl -a** para listar os valores de parâmetro.
   b. Analise os resultados usando as diretrizes em Tabela 13 para determinar se quaisquer mudanças são necessárias.
   c. Se as mudanças forem necessárias, configure os parâmetros no arquivo `/etc/sysctl.conf`. As mudanças no arquivo são aplicadas quando o sistema é iniciado.

   Dica: Ajustar automaticamente as configurações de parâmetro do kernel e eliminar a necessidade de atualizações manuais para essas configurações. No Linux, o Db2 software de banco de dados ajusta automaticamente os valores de parâmetro do kernel de comunicação interprocessual (IPC) para as configurações preferenciais. Para obter informações adicionais sobre configurações de parâmetro do kernel, procure parâmetros do kernel Linux no Documentação do produto IBM Db2 versão 11.1.

Tabela 13. Configurações ideais de parâmetro do kernel do Linux

Parâmetro	descrição
kernel.shmmni	O número máximo de segmentos.
kernel.shmmax	O tamanho máximo de um segmento de memória compartilhada (bytes). Este parâmetro deve ser configurado antes do início automático do servidor do IBM Spectrum Protect na inicialização do sistema.
kernel.shmall	A alocação máxima das páginas de memória compartilhada (páginas).
kernel.sem Há quatro valores para o parâmetro **kernel.sem**.	(SEMMSL) O máximo de semáforos por matriz.
	(SEMMNS) O máximo de semáforos por sistema.
	(SEMOPM) O máximo de operações por chamada de semáforo.
	(SEMMNI) O número máximo de matrizes.
kernel.msgmni	O número máximo de filas de mensagens de todo o sistema.
kernel.msgmax	O tamanho máximo de mensagens (bytes).
kernel.msgmnb	O tamanho máximo padrão da fila (bytes).
kernel.randomize_va_space	O parâmetro **kernel.randomize_va_space** configura o uso da memória ASLR para o kernel. Ative o ASLR para a V7.1 e para servidores posteriores. Para saber mais detalhes sobre o Linux ASLR e o Db2, consulte a nota técnica 1365583.
vm.swappiness	O parâmetro **vm.swappiness** define se o kernel pode descarregar a memória do aplicativo na memória de acesso aleatório (RAM) física. Para obter informações adicionais sobre os parâmetros do kernel, consulte o Informações do produto Db2.

Tabela 13. Configurações ideais de parâmetro do kernel do Linux (continuação)

Parâmetro	descrição
vm.overcommit_memory	O parâmetro **vm.overcommit_memory** influencia quanta memória virtual o kernel permite alocar. Para obter informações adicionais sobre os parâmetros do kernel, consulte o Informações do produto Db2.

7. Abra as portas de firewall para se comunicar com o servidor. Execute as etapas a seguir:
   a. Determine a zona usada pela interface de rede. Por padrão, a zona é pública.

      Emita o seguinte comando:

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b. Para usar o endereço de porta padrão para comunicações com o servidor, abra a porta TCP/IP 1500 no firewall Linux.

      Emita o seguinte comando:

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

      Se desejar usar um valor diferente do padrão, é possível especificar um número no intervalo de 1024 a 32767. Se você abrir uma porta diferente do padrão, será necessário especificar essa porta quando executar o script de configuração.

   c. Se você planeja usar esse sistema como um hub, abra a porta 11090, que é a porta padrão para comunicações seguras (https).

      Emita o seguinte comando:

      ```
      firewall-cmd --zone=public --add-port=11090/tcp --permanent
      ```

   d. Recarregue as definições de firewall para que as mudanças entrem em vigor.

      Emita o seguinte comando:

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

8. Verifique se os limites de recurso do processo do usuário, também conhecidos como *ulimits*, estão configurados de acordo com as diretrizes em Tabela 14. Se os valores de ulimit não estiverem configurados corretamente, pode haver instabilidade do servidor ou uma falha do servidor ao responder.

Tabela 14. Valores de limites do usuário (ulimit)

Tipo de limite do usuário	Configuração	Valor	Comando para consultar valor
Tamanho máximo dos arquivos principais criados	`core`	Sem limites	`ulimit -Hc`
Tamanho máximo de um segmento de dados para um processo	`dados`	Sem limites	`ulimit -Hd`
Tamanho máximo do arquivo	`fsize`	Sem limites	`ulimit -Hf`
Número máximo de arquivos abertos	`nofile`	65536	`ulimit -Hn`

Tabela 14. Valores de limites do usuário (ulimit) (continuação)

Tipo de limite do usuário	Configuração	Valor	Comando para consultar valor
Quantidade máxima de tempo do processador em segundos	`cpu`	Sem limites	`ulimit -Ht`
Número máximo de processos do usuário	`nproc`	16384	`ulimit -Hu`

Se precisar modificar quaisquer valores de limite do usuário, siga as instruções na documentação de seu sistema operacional.

Instalando em sistemas Windows

Instale o Microsoft Windows Server 2012 Standard Edition no sistema do servidor e prepare o sistema para instalação e configuração do servidor do IBM Spectrum Protect.

Procedimento

1. Instale o Windows Server 2016 Standard Edition de acordo com as instruções do fabricante.
2. Altere as políticas de controle de conta do Windows concluindo as etapas a seguir.
   a. Abra o editor Política de segurança local executando `secpol.msc`.
   b. Clique em **Políticas locais** > **Opções de segurança** e assegure-se de que as políticas de Controle de conta do usuário a seguir estejam desativadas:
      - Modo de aprovação de administrador para a conta do Administrador integrado
      - Execute todos os administradores no Modo de aprovação de administrador
3. Defina as configurações de TCP/IP de acordo com as instruções de instalação para o sistema operacional.
4. Aplique atualizações do Windows e ative recursos opcionais concluindo as etapas a seguir:
   a. Aplique as atualizações mais recentes do Windows Server 2016.
   b. Instale e ative o recurso Microsoft .NET Framework 3.5 do Windows 2012 R2 a partir do Windows Server Manager.
   c. Se necessário, atualize os drivers de dispositivo HBA FC e Ethernet para níveis mais recentes.
   d. Instale o driver de E/S de caminhos múltiplos que seja apropriado para o sistema de disco que está sendo usado.
5. Abra a porta TCP/IP padrão, 1500, para comunicações com o servidor do IBM Spectrum Protect. Por exemplo, emita o seguinte comando:

   ```
   netsh advfirewall firewall add rule name="Backup server port 1500"
   dir=in action=allow protocol=TCP localport=1500
   ```

6. No servidor do hub do Operations Center, abra a porta padrão para comunicações seguras (https) com o Operations Center. O número da porta é 11090. Por exemplo, emita o seguinte comando:

   ```
   netsh advfirewall firewall add rule name="Operations Center port 11090"
   dir=in action=allow protocol=TCP localport=11090
   ```

Configurando a E/S de caminhos múltiplos

É possível ativar e configurar caminhos múltiplos para armazenamento em disco. Use a documentação que é fornecida com seu hardware para obter instruções detalhadas.

Sistemas AIX

Procedimento

1. Determine o endereço de porta Fibre Channel que deve ser usado para a definição de host no subsistema de disco. Emita o comando **lscfg** para cada porta.
   - Em sistemas pequenos e médios, emita os seguintes comandos:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     ```

   - Em sistemas grandes, emita os seguintes comandos:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     lscfg -vps -l fcs2 | grep "Network Address"
     lscfg -vps -l fcs3 | grep "Network Address"
     ```

2. Certifique-se de que os seguintes conjuntos de arquivos do AIX estejam instalados:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Emita o comando **cfgmgr** para que o AIX varra novamente o hardware e descubra os discos disponíveis. Por exemplo:

   ```
   cfgmgr
   ```

4. Para listar os discos disponíveis, emita o seguinte comando:

   ```
   lsdev -Ccdisk
   ```

   Você deve ver uma saída semelhante à seguinte:

   ```
   hdisk0  Available 00-00-00 SAS Disk Drive
   hdisk1  Available 00-00-00 SAS Disk Drive
   hdisk2  Available 01-00-00 SAS Disk Drive
   hdisk3  Available 01-00-00 SAS Disk Drive
   hdisk4  Available 06-01-02 MPIO IBM 2076 FC Disk
   hdisk5  Available 07-01-02 MPIO IBM 2076 FC Disk
   ...
   ```

5. Use a saída do comando **lsdev** para identificar e listar IDs de dispositivos para cada dispositivo de disco.

   Por exemplo, um ID do dispositivo pode ser `hdisk4`. Salve a lista de IDs de dispositivos a ser usada ao criar sistemas de arquivos para o servidor do IBM Spectrum Protect.
6. Correlacione os IDs de dispositivos SCSI com LUNs de disco específicos do sistema de disco, listando informações detalhadas sobre todos os volumes físicos no sistema. Emita o seguinte comando:

   ```
   lspv -u
   ```

   Em um sistema IBM Storwize, as informações a seguir são um exemplo do que é mostrado para cada dispositivo:

   ```
   hdisk4  00f8cf083fd97327  None  active
    3321360050763008101057800000000000030042145O3IBMfcp
   ```

No exemplo, *600507630081010578000000000000030* é o UID do volume, conforme relatado pela interface de gerenciamento do Storwize.

Para verificar o tamanho do disco em megabytes e comparar o valor com o que estiver listado para o sistema, emita o comando a seguir:

```
bootinfo -s hdisk4
```

Sistemas Linux

Procedimento

1. Edite o arquivo `/etc/multipath.conf` para ativar caminhos múltiplos para hosts do Linux. Se o arquivo `multipath.conf` não existir, é possível criá-lo emitindo o seguinte comando:

   ```
   mpathconf --enable
   ```

   Os parâmetros a seguir foram configurados em `multipath.conf` para testar em um sistema IBM Storwize:

   ```
   defaults {
         user_friendly_names no
   }

   devices {
         device {
               vendor "IBM "
               product "2145"
               path_grouping_policy group_by_prio
               user_friendly_names no
               path_selector "round-robin 0"
               Prioridade "alua"
               path_checker "tur"
               retorno "imediato"
               no_path_retry 5
               rr_weight uniform
               rr_min_io_rq "1"
               dev_loss_tmo 120
        }
   }
   ```

2. Configure a opção de caminhos múltiplos para iniciar quando o sistema for iniciado. Emita os seguintes comandos:

   ```
   systemctl enable multipathd.service
   systemctl start multipathd.service
   ```

3. Para verificar se os discos estão visíveis para o sistema operacional e são gerenciados por caminhos múltiplos, emita o seguinte comando:

   ```
   multipath -l
   ```

4. Certifique-se de que cada dispositivo esteja listado e que tenha a quantidade de caminhos esperada. É possível usar informações de tamanho e de ID do dispositivo para identificar quais discos estão listados.

   Por exemplo, a seguinte saída mostra que um disco de 2 TB possui dois grupos de caminhos e quatro caminhos ativos. O tamanho de 2 TB confirma que o disco corresponde a sistema de arquivos do conjunto. Use parte do número do ID do dispositivo longo (12, nesse exemplo) para procurar o volume na interface de gerenciamento de sistemas de disco.

   ```
   [root@tapsrv01 code]# multipath -l
   36005076802810c509800000000000012 dm-43 IBM,2145
    size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=0 status=active
   | |- 2:0:1:18 sdcw 70:64   active undef running
   | `- 4:0:0:18 sdgb 131:112 active undef running
   ```

```
`-+- policy='round-robin 0' prio=0 status=enabled
  |- 1:0:1:18 sdat 66:208  active undef running
  `- 3:0:0:18 sddy 128:0   active undef running
```

a. Se necessário, corrija as designações de host do LUN de disco e force uma nova varredura de barramento. Por exemplo:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

Também é possível reiniciar o sistema para varrer novamente as designações de host do LUN de disco.

b. Confirme se os discos agora estão disponíveis para E/S de caminhos múltiplos emitindo novamente o comando **multipath -l**.

5. Use a saída de caminhos múltiplos para identificar e listar IDs de dispositivos para cada dispositivo de disco.

   Por exemplo, o ID do dispositivo para seu disco de 2 TB é 36005076802810c509800000000000012.

   Salve a lista de IDs de dispositivos para usar na próxima etapa.

Sistemas Windows

Procedimento

1. Certifique-se de que o recurso E/S de Caminhos Múltiplos esteja instalado. Se necessário, instale drivers de caminhos múltiplos adicionais específicos do fornecedor.
2. Para verificar se os discos estão visíveis para o sistema operacional e são gerenciados por E/S de caminhos múltiplos, emita o seguinte comando:

   ```
   c:\program files\IBM\SDDDSM\datapath.exe query device
   ```

3. Revise a saída de caminhos múltiplos e certifique-se de que cada dispositivo esteja listado e tenha a quantidade de caminhos esperada. É possível usar informações de tamanho e de série do dispositivo para identificar quais discos estão listados.

   Por exemplo, usando parte do número de série longo do dispositivo (34, nesse exemplo), é possível procurar o volume na interface de gerenciamento de sistemas de disco. O tamanho de 2 TB confirma que o disco corresponde a um sistema de arquivos do conjunto de armazenamentos.

```
DEV#:   4  DEVICE NAME: Disk5 Part0   TYPE: 2145    POLICY: OPTIMIZED
SERIAL: 600507630081010578000000000000034          LUN SIZE: 2.0TB
============================================================================
Path#          Adapter/Hard Disk       State   Mode    Select  Errors
    0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
    1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
    2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
    3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
```

4. Crie uma lista de IDs de dispositivo de disco usando os números de série que são retornados da saída de caminhos múltiplos na etapa anterior.

   Por exemplo, o ID do dispositivo para seu disco de 2 TB é 600507630081010578000000000000034

   Salve a lista de IDs de dispositivos para usar na próxima etapa.

5. Para colocar novos discos on-line e limpar o atributo de leitura, execute diskpart.exe com os seguintes comandos. Repita para cada um dos discos:

```
diskpart
   select Disk 1
   online disk
```

```
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

Criando o ID do usuário para o servidor

Crie o ID do usuário que possui a instância do servidor IBM Spectrum Protect. Você especifica esse ID do usuário ao criar a instância do servidor durante a configuração inicial do servidor.

Sobre Esta Tarefa

É possível especificar apenas letras minúsculas (a-z), numerais (0-9) e o caractere de sublinhado (_) para o ID do usuário. O ID do usuário e o nome do grupo devem estar em conformidade com as seguintes regras:

- O comprimento deve ser 8 caracteres ou menos.
- Não podem iniciar com *ibm*, *sql*, *sys* ou numeral.
- O ID do usuário e o nome do grupo não podem ser *user*, *admin*, *guest*, *public*, *local* ou qualquer palavra reservada de SQL.

Procedimento

1. Use comandos do sistema operacional para criar um ID do usuário.
   - AIX Linux Crie um grupo e um ID do usuário no diretório inicial do usuário que possui a instância do servidor.

     Por exemplo, para criar o ID do usuário `tsminst1` no grupo `tsmsrvrs` com uma senha de `tsminst1`, emita os seguintes comandos a partir de um ID do usuário administrativo:

     AIX

     ```
     mkgroup id=1001 tsmsrvrs
     mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
     passwd tsminst1
     ```

     Linux

     ```
     groupadd
     tsmsrvrs
     useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
     passwd tsminst1
     ```

     Efetue logoff e, em seguida, efetue login em seu sistema. Mude para a conta do usuário que você criou. Use um programa de login interativo, como telnet, para que você solicite a senha e possa alterá-la se necessário.
   - Windows Crie um ID do usuário e, em seguida, inclua o novo ID no grupo de Administradores. Por exemplo, para criar o ID do usuário `tsminst1`, emita o seguinte comando:

     ```
     net user tsminst1 * /add
     ```

     Após criar e verificar uma senha para o novo usuário, inclua o ID do usuário no grupo de Administradores emitindo os seguintes comandos:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Efetue logoff no novo ID do usuário.

Preparando sistemas de arquivos para o servidor

Deve-se concluir a configuração do sistema de arquivos para o armazenamento em disco a ser usado pelo servidor.

Sistemas AIX

Deve-se criar grupos lógicos, volumes lógicos e sistemas de arquivos para o servidor usando o Gerenciador de Volume Lógico AIX.

Procedimento

1. Aumente a profundidade da fila e o tamanho máximo de transferência para todos os discos *hdiskX* disponíveis. Emita os seguintes comandos para cada disco:

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   Não execute esses comandos para discos internos do sistema operacional, por exemplo, *hdisk0*.

2. Crie grupos de volumes para o banco de dados, log ativo, log de archive, backup de banco de dados e conjunto de armazenamentos do IBM Spectrum Protect. Emita o comando **mkvg**, especificando os IDs do dispositivo para discos correspondentes que foram identificados anteriormente.

   Por exemplo, se os nomes de dispositivos *hdisk4*, *hdisk5* e *hdisk6* corresponderem a discos do banco de dados, inclua-os no grupo de volumes do banco de dados e assim por diante.

   Tamanho do sistema: Os seguintes comandos são baseados na configuração do sistema médio. Para sistemas pequenos e grandes, deve-se ajustar a sintaxe conforme necessário.

   ```
   mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
   mkvg -S -y tsmactlog hdisk5
   mkvg -S -y tsmarchlog hdisk6
   mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
   mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
   ```

3. Determine os nomes de volumes físicos e o número de partições físicas livres a serem usadas ao criar volumes lógicos. Emita **lsvg** para cada grupo de volumes criado na etapa anterior.

   Por exemplo:

   ```
   lsvg -p tsmdb
   ```

   A saída é semelhante à seguinte. A coluna *FREE PPs* representa as três partições físicas livres:

   ```
   tsmdb:
   PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4   active     1631       1631      327..326..326..326..326
   hdisk5   active     1631       1631      327..326..326..326..326
   hdisk6   active     1631       1631      327..326..326..326..326
   ```

4. Crie volumes lógicos em cada grupo de volumes usando o comando **mklv**. O tamanho do volume, o grupo de volumes e os nomes dos dispositivos variam, dependendo do tamanho do seu sistema e de variações na configuração do disco.

   Por exemplo, para criar os volumes para o banco de dados do IBM Spectrum Protect em um sistema médio, emita os seguintes comandos:

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. Formate sistemas de arquivos em cada volume lógico usando o comando **crfs**.

   Por exemplo, para formatar sistemas de arquivos para o banco de dados em um sistema médio, emita os seguintes comandos:

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

6. Monte todos os sistemas de arquivos recém-criados emitindo o seguinte comando:

   ```
   mount -a
   ```

7. Liste todos os sistemas de arquivos emitindo o comando **df**. Verifique se os sistemas de arquivos estão montados no LUN correto e no ponto de montagem correto. Verifique também o espaço disponível.

   O exemplo de saída de comando a seguir mostra que a quantia de espaço usado geralmente é 1%:

   ```
   tapsrv07> df -g /tsminst1/*
   Filesystem      GB blocks  Free     %Used   Iused   %Iused   Mounted on
   /dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
   ```

8. Verifique se o ID do usuário criado em "Criando o ID do usuário para o servidor" na página 48 possui acesso de leitura e gravação aos diretórios para o servidor do IBM Spectrum Protect.

Sistemas Linux

Deve-se formatar sistemas de arquivos `ext4` ou `xfs` em cada um dos LUNs de disco a ser usado pelo servidor do IBM Spectrum Protect.

Procedimento

1. Usando a lista de IDs de dispositivos que você gerou anteriormente, emita o comando **mkfs** para criar e formatar um sistema de arquivos para cada dispositivo LUN de armazenamento. Especifique o ID do dispositivo no comando. Consulte os exemplos a seguir. Para o banco de dados, formate os sistemas de arquivos `ext4`:

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Para LUNs do conjunto de armazenamentos, formate os sistemas de arquivos `xfs`:

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

   É possível emitir o comando **mkfs** até 50 vezes, dependendo de quantos dispositivos diferentes você possui.

2. Crie diretórios de ponto de montagem para sistemas de arquivos.

Emita o comando **mkdir** para cada diretório que você deve criar. Use os valores de diretório registrados nas planilhas de planejamento. Por exemplo, para criar o diretório de instância do servidor usando o valor padrão, emita o seguinte comando:

```
mkdir /tsminst1
```

Repita o comando **mkdir** para cada sistema de arquivos.

3. Inclua uma entrada no arquivo `/etc/fstab` para cada sistema de arquivos para que os sistemas de arquivos sejam montados automaticamente quando o servidor for iniciado.

   Por exemplo:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Monte os sistemas de arquivos que foram incluídos no arquivo `/etc/fstab` emitindo o comando **mount -a**.
5. Liste todos os sistemas de arquivos emitindo o comando **df**. Verifique se os sistemas de arquivos estão montados no LUN correto e no ponto de montagem correto. Verifique também o espaço disponível.

   O exemplo a seguir em um sistema IBM Storwize mostra que a quantia de espaço usado geralmente é 1%:

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Filesystem                                      Size  Used Avail Use% Mounted on
   /dev/mapper/3600507630081010578000000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
   ```

6. Verifique se o ID do usuário criado em "Criando o ID do usuário para o servidor" na página 48 tem acesso de leitura e gravação aos diretórios para o IBM Spectrum Protect.

Sistemas Windows

Deve-se formatar sistemas de arquivos NTFS em cada um dos LUNs de disco a serem usados pelo servidor do IBM Spectrum Protect.

Procedimento

1. Crie diretórios de ponto de montagem para sistemas de arquivos.

   Emita o comando **md** para cada diretório que você deve criar. Use os valores de diretório registrados nas planilhas de planejamento. Por exemplo, para criar o diretório de instância do servidor usando o valor padrão, emita o seguinte comando:

   ```
   md c:\tsminst1
   ```

   Repita o comando **md** para cada sistema de arquivos.

2. Crie um volume para cada LUN de disco que é mapeado para um diretório no diretório de instância do servidor usando o gerenciador de volume do Windows.

   Acesse **Gerenciador do servidor** > **Serviços de arquivo e armazenamento** e conclua as etapas a seguir para cada disco que corresponda ao mapeamento de LUN que foi criado na etapa anterior:

   a. Torne o disco online.
   b. Inicialize o disco para o tipo básico de GPT, que é o padrão.
   c. Crie um volume simples que ocupe todo o espaço no disco. Formate o sistema de arquivos usando NTFS e designe um rótulo que corresponda ao propósito do volume, como `TSMfile00`. Não designe o novo volume a uma letra da unidade. Em vez disso, mapeie o volume para um diretório no diretório de instâncias, como `C:\tsminst1\TSMfile00`.

Dica: Determine o rótulo de volume e os rótulos de mapeamento de volume com base no tamanho do disco relatado.

3. Verifique se os sistemas de arquivos estão montados no LUN correto e no ponto de montagem correto. Liste todos os sistemas de arquivos emitindo o comando **mountvol** e, em seguida, revise a saída. Por exemplo:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
  C:\tsminst1\TSMdbspace00\
```

4. Após a conclusão da configuração do disco, reinicie o sistema.

O que Fazer Depois

É possível confirmar a quantidade de espaço livre para cada volume usando o Windows Explorer.

Capítulo 8. Instalando o servidor e o Operations Center

Use o assistente gráfico do IBM Installation Manager para instalar os componentes.

Instalando em sistemas AIX e Linux

Instale o servidor do IBM Spectrum Protect e o Operations Center no primeiro sistema de servidor.

Antes de Iniciar

Verifique se o sistema operacional está configurado para o idioma que você precisa. Por padrão, o idioma do sistema operacional é o idioma do assistente de instalação.

Procedimento

1. AIX Verifique se os arquivos RPM necessários estão instalados em seu sistema.

   Consulte “Instalando arquivos RPM de pré-requisito para o assistente gráfico” na página 54 para obter mais detalhes.
2. Antes de fazer download do pacote de instalação, verifique se há espaço suficiente para armazenar os arquivos de instalação quando eles forem extraídos do pacote do produto. Para obter os requisitos de espaço, consulte o documento de download em nota técnica 4042992.
3. Acesse Passport Advantage e faça download do arquivo de pacote para um diretório vazio de sua escolha.
4. Certifique-se de que a permissão executável esteja configurada para o pacote. Se necessário, altere as permissões de arquivo, emitindo o comando a seguir:

   ```
   chmod a+x package_name.bin
   ```
5. Extraia o pacote emitindo o seguinte comando:

   ```
   ./package_name.bin
   ```

   em que *package_name* é o nome do arquivo transferido por download.
6. AIX Assegure-se de que o comando a seguir esteja ativado para que os assistentes funcionem adequadamente:

   ```
   lsuser
   ```

   Por padrão, o comando está ativado.
7. Vá para o diretório onde colocou o arquivo executável.
8. Inicie o assistente de instalação emitindo o seguinte comando:

   ```
   ./install.sh
   ```

   Ao selecionar os pacotes para instalar, escolha o servidor e o Operations Center.

O que Fazer Depois

- Se ocorrerem erros durante o processo de instalação, esses erros serão registrados nos arquivos de log armazenados no diretório de logs do IBM Installation Manager.

Para visualizar arquivos de log de instalação da ferramenta do Installation Manager, clique em **Arquivo** > **Visualizar log**. Para coletar esses arquivos de log da ferramenta do Installation Manager, clique em **Ajuda** > **Exportar dados para análise de problemas**.

- Após instalar o servidor e antes de customizá-lo para seu uso, acesse Site de Suporte do IBM Spectrum Protect. Clique em **Suporte e Downloads** e aplique todas as correções aplicáveis.

Tarefas relacionadas:

Outros métodos para instalar componentes do IBM Spectrum Protect (AIX)

Outros métodos para instalar componentes do IBM Spectrum Protect (Linux)

Instalando arquivos RPM de pré-requisito para o assistente gráfico

AIX

Os arquivos RPM são necessários para o assistente gráfico do IBM Installation Manager.

Procedimento

1. Verifique se os seguintes arquivos estão instalados no sistema. Se os arquivos não estiverem instalados, acesse a Etapa 2.

```
atk-1.12.3-2.aix5.2.ppc.rpm
cairo-1.8.8-1.aix5.2.ppc.rpm
expat-2.0.1-1.aix5.2.ppc.rpm
fontconfig-2.4.2-1.aix5.2.ppc.rpm
freetype2-2.3.9-1.aix5.2.ppc.rpm
gettext-0.10.40-6.aix5.1.ppc.rpm
glib2-2.12.4-2.aix5.2.ppc.rpm
gtk2-2.10.6-4.aix5.2.ppc.rpm
libjpeg-6b-6.aix5.1.ppc.rpm
libpng-1.2.32-2.aix5.2.ppc.rpm
libtiff-3.8.2-1.aix5.2.ppc.rpm
pango-1.14.5-4.aix5.2.ppc.rpm
pixman-0.12.0-3.aix5.2.ppc.rpm
xcursor-1.1.7-3.aix5.2.ppc.rpm
xft-2.1.6-5.aix5.1.ppc.rpm
xrender-0.9.1-3.aix5.2.ppc.rpm
zlib-1.2.3-3.aix5.1.ppc.rpm
```

2. Assegure-se de que haja pelo menos 150 MB de espaço livre no sistema de arquivos `/opt`.
3. No diretório em que o pacote de instalação foi extraído, acesse o diretório `gtk`.
4. Faça download dos arquivos RPM para o diretório atualmente em funcionamento do website IBM AIX Toolbox for Linux Applications emitindo o seguinte comando:

```
download-prerequisites.sh
```

5. No diretório que contém os arquivos RPM transferidos por download, instale-os emitindo o seguinte comando:

```
rpm -Uvh *.rpm
```

Instalando em sistemas Windows

Instale o servidor do IBM Spectrum Protect e o Operations Center no primeiro sistema de servidor.

Antes de Iniciar

Certifique-se de que os seguintes requisitos sejam atendidos:

- Verifique se o sistema operacional está configurado para o idioma que você precisa. Por padrão, o idioma do sistema operacional é o idioma do assistente de instalação.

- Certifique-se de que o ID do usuário que você planeja usar durante a instalação seja um usuário com autoridade do Administrador local.

Procedimento

1. Antes de fazer download do pacote de instalação, verifique se há espaço suficiente para armazenar os arquivos de instalação quando eles forem extraídos do pacote do produto. Para obter os requisitos de espaço, consulte o documento de download em nota técnica 4042993.
2. Acesse Passport Advantage e faça download do arquivo de pacote para um diretório vazio de sua escolha.
3. Vá para o diretório onde colocou o arquivo executável.
4. Dê um clique duplo no arquivo executável para extrair para o diretório atual.
5. No diretório em que os arquivos de instalação foram extraídos, inicie o assistente de instalação dando um clique duplo no arquivo `install.bat`. Ao selecionar os pacotes para instalar, escolha o servidor e o Operations Center.

O que Fazer Depois

- Se ocorrerem erros durante o processo de instalação, esses erros serão registrados nos arquivos de log armazenados no diretório de logs do IBM Installation Manager.

  Para visualizar arquivos de log de instalação da ferramenta do Installation Manager, clique em **Arquivo** > **Visualizar log**. Para coletar esses arquivos de log da ferramenta do Installation Manager, clique em **Ajuda** > **Exportar dados para análise de problemas**.
- Após instalar o servidor e antes de customizá-lo para seu uso, acesse Site de Suporte do IBM Spectrum Protect. Clique em **Suporte e Downloads** e aplique todas as correções aplicáveis.

Tarefas relacionadas:

Outros métodos para instalação de componentes do IBM Spectrum Protect

Capítulo 9. Configurando o servidor e o Operations Center

Depois de instalar os componentes, conclua a configuração para o servidor IBM Spectrum Protect e o Operations Center.

Configurando a instância do servidor

Use o assistente de configuração da instância do servidor do IBM Spectrum Protect para concluir a configuração inicial do servidor.

Antes de Iniciar

Certifique-se de que os requisitos a seguir sejam atendidos:

AIX Linux

- O sistema em que você instalou o IBM Spectrum Protect deve ter o cliente X Window System. Você deve também estar executando um servidor X Window System em seu desktop.
- O sistema deve ter o protocolo Shell Seguro (SSH) ativado. Certifique-se de que a porta esteja configurada para o valor padrão, 22, e que a porta não esteja bloqueada por um firewall. É necessário ativar a autenticação de senha no arquivo `sshd_config` no diretório `/etc/ssh/`. Além disso, certifique-se de que o serviço de daemon SSH tenha direitos de acesso para conectar-se ao sistema usando o valor *localhost*.
- É necessário poder efetuar login no IBM Spectrum Protect com o ID do usuário criado para a instância do servidor, usando o protocolo SSH. Ao usar o assistente, é necessário fornecer este ID do usuário e a senha para acessar esse sistema.
- Se você mudou alguma configuração nas etapas anteriores, reinicie o servidor antes de continuar com o assistente de configuração.

Windows Verifique se o serviço de registro remoto foi iniciado concluindo as etapas a seguir:

1. Clique em **Iniciar** > **Ferramentas administrativas** > **Serviços**. Na janela Serviços, selecione **Registro remoto**. Se ele não estiver iniciado, clique em **Iniciar**.
2. Assegure-se de que as portas 137, 139 e 445 não estejam bloqueadas por um firewall:
   a. Clique em **Iniciar** > **Painel de controle** > **Windows Firewall**.
   b. Selecione **Configurações avançadas**.
   c. Selecione **Regras de Entrada**.
   d. Selecione **Nova regra**.
   e. Crie uma regra de porta para as portas TCP 137, 139 e 445 para permitir conexões para redes de domínio e privadas.
3. Configure o controle de conta do usuário acessando as opções de política de segurança local e concluindo as etapas a seguir.
   a. Clique em **Iniciar** > **Ferramentas administrativas** > **Política de segurança local**. Expanda **Políticas locais** > **Opções de segurança**.

b. Se ainda não estiver ativada, ative a conta do administrador integrado, selecionando **Contas: Status da conta do administrador** > **Ativar** > **OK**.

c. Se ainda não estiver desativado, desative o controle de conta do usuário para todos os administradores do Windows, selecionando **Controle de conta do usuário: executar todos os administradores no modo de aprovação de administrador** > **Desativar** > **OK**.

d. Se ainda não estiver desativado, desative o Controle de conta do usuário para a conta do Administrador integrado, selecionando **Controle de conta do usuário: modo de aprovação do administrador para a conta do administrador integrado** > **Desativar** > **OK**.

4. Se você mudou alguma configuração nas etapas anteriores, reinicie o servidor antes de continuar com o assistente de configuração.

Sobre Esta Tarefa

O assistente pode ser interrompido e reiniciado, mas o servidor não estará operacional até que todo o processo de configuração esteja concluído.

Procedimento

1. Inicie a versão local do assistente.
   - AIX Linux Abra o programa `dsmicfgx` no diretório `/opt/tivoli/tsm/server/bin`. Este assistente pode ser executado somente como um usuário raiz.
   - Windows Clique em **Iniciar** > **Todos os programas** > **IBM Spectrum Protect** > **Assistente de configuração**.
2. Siga as instruções para concluir a configuração. Use as informações registradas no Capítulo 4, “Planilhas de planejamento”, na página 13 durante a configuração do sistema IBM Spectrum Protect para especificar diretórios e opções no assistente.

   AIX Linux Na janela Informações do servidor, configure o servidor para iniciar automaticamente usando o ID do usuário da instância quando o sistema for inicializado.

   Windows Usando o assistente de configuração, o servidor é configurado para iniciar automaticamente quando reinicializado.

Instalando o cliente de backup-archive

Como uma melhor prática, instale o cliente de backup-archive do IBM Spectrum Protect no sistema do servidor para que o cliente da linha de comando administrativo e o planejador estejam disponíveis.

Procedimento

Para instalar o cliente de backup-archive, siga as instruções de instalação para seu sistema operacional.

- Instale deus clientes de archive de backup do UNIX e do Linux
- Instalando o cliente Windows pela primeira vez

Configurando opções para o servidor

Revise o arquivo de opções do servidor que está instalado com o servidor do IBM Spectrum Protect para verificar se os valores corretos estão configurados para seu sistema.

Procedimento

1. Acesse o diretório de instância do servidor e abra o arquivo `dsmserv.opt`.
2. Revise os valores na tabela a seguir e verifique as configurações de opção do servidor, com base no tamanho do sistema.

Opção do servidor	Valor do sistema pequeno	Valor do sistema médio	Valor do sistema grande
ACTIVELOGDIRECTORY	Caminho do diretório especificado durante a configuração	Caminho do diretório especificado durante a configuração	Caminho do diretório especificado durante a configuração
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	SIM	Sim	Sim
ARCHLOGDIRECTORY	Caminho do diretório especificado durante a configuração	Caminho do diretório especificado durante a configuração	Caminho do diretório especificado durante a configuração
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	Sim	Sim	Sim
DEVCONFIG	`devconf.dat`	`devconf.dat`	`devconf.dat`
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	`volhist.dat`	`volhist.dat`	`volhist.dat`

   Atualize as configurações de opção do servidor, se necessário, para que correspondam aos valores na tabela. Para fazer atualizações, feche o arquivo `dsmserv.opt` e use o comando **SETOPT** a partir da interface da linha de comandos administrativa para configurar as opções.

   Por exemplo, para atualizar a opção `IDLETIMEOUT` para 60, emita o seguinte comando:

   ```
   setopt idletimeout 60
   ```

3. Para configurar comunicações seguras para o servidor, clientes e o Operations Center, verifique as opções na tabela a seguir.

Opção do servidor	Todos os tamanhos do sistema
SSLFIPSMODE	NO

Opção do servidor	Todos os tamanhos do sistema
TCPPORT	Especifique o número da porta na qual o servidor espera solicitações de sessões ativadas para TCP/IP e SSL do cliente.
TCPADMINPORT	Especifique o endereço de porta no qual o servidor espera solicitações de sessões ativadas para TCP/IP e SSL do cliente administrador da linha de comandos.

Se algum dos valores da opção tiver que ser atualizado, edite o arquivo `dsmserv.opt` usando as seguintes diretrizes:

- Remova o asterisco no início de uma linha para ativar uma opção.
- Em cada linha, insira apenas uma opção e o valor especificado para a opção.
- Se uma opção ocorrer em diversas entradas no arquivo, o servidor usará a última entrada.

Salve suas mudanças e feche o arquivo. Se você editar o arquivo `dsmserv.opt` diretamente, será necessário reiniciar o servidor para que as mudanças entrem em vigor.

Referências relacionadas:

Referência de opções do servidor

SETOPT (Definir uma opção do servidor para atualização dinâmica)

Configurando comunicações seguras com a Segurança da Camada de Transporte

Para criptografar os dados e as comunicações seguras em seu ambiente, o Secure Sockets Layer (SSL) ou a Segurança da Camada de Transporte (TLS) é ativada no servidor IBM Spectrum Protect e no cliente de backup-archive. Um certificado SSL é usado para verificar solicitações de comunicação entre o servidor e o cliente.

Sobre Esta Tarefa

A partir do IBM Spectrum Protect Versão 8.1.2, o SSL é ativado por padrão e o servidor IBM Spectrum Protect e o cliente de backup-archive são configurados automaticamente para se comunicarem usando o protocolo TLS 1.2.

Conforme mostrado na figura a seguir, é possível configurar manualmente as comunicações seguras entre o servidor e o cliente de backup-archive, configurando opções nos arquivos de opções do servidor e do cliente e, em seguida, transferindo o certificado autoassinado, que é gerado no servidor, para o cliente. Como alternativa, é possível obter e transferir um certificado exclusivo que é assinado por uma autoridade de certificação (CA).

Para obter mais informações sobre como configurar o servidor e os clientes para comunicações de SSL ou de TLS, consulte Configurando agentes de armazenamento, servidores, clientes e o Operations Center para se conectar ao servidor usando SSL.

Configurando o Operations Center

Após instalar o Operations Center, conclua as etapas a seguir de configuração para começar a gerenciar seu ambiente de armazenamento.

Antes de Iniciar

Ao conectar-se ao Operations Center pela primeira vez, é necessário fornecer as informações a seguir:

- Informações de conexão para o servidor que deseja designar como um servidor do hub
- Credenciais de login para um ID de administrador que está definido para esse servidor

Procedimento

1. Designe o servidor do hub. Em um navegador da web, insira o seguinte endereço:

   `https://hostname:secure_port/oc`

   onde:

   - *hostname* representa o nome do computador no qual o Operations Center está instalado
   - *secure_port* representa o número da porta que o Operations Center usa para comunicação HTTPS nesse computador

   Por exemplo, se seu nome do host for tsm.storage.mylocation.com e você estiver usando a porta segura padrão para o Operations Center, que é 11090, o endereço será:

   `https://tsm.storage.mylocation.com:11090/oc`

   Ao efetuar login no Operations Center pela primeira vez, um assistente o orienta por uma configuração inicial para configurar um novo administrador com autoridade do sistema no servidor.

2. Configure as comunicações seguras entre o Operations Center e o servidor do hub configurando o protocolo Secure Sockets Layer (SSL).

   Siga as instruções em “Protegendo as comunicações entre o Operations Center e o servidor do hub”.
3. Opcional: Para receber um relatório de email diário que resume o status do sistema, defina suas configurações de email no Operations Center.

   Siga as instruções em Capítulo 16, “Rastreando o status do sistema usando relatórios de e-mail”, na página 103.

Protegendo as comunicações entre o Operations Center e o servidor do hub

Para proteger as comunicações entre o Operations Center e o servidor do hub, inclua o certificado Segurança da Camada de Transporte (TLS) do servidor do hub no arquivo de armazenamento confiável do Operations Center.

Antes de Iniciar

O arquivo de armazenamento confiável do Operations Center é um contêiner para certificados que o Operations Center pode acessar. Ele contém o certificado que o Operations Center usa para comunicação HTTPS com navegadores da web.

Durante a instalação do Operations Center, crie uma senha para o arquivo de armazenamento confiável. Para proteger a comunicação entre o Operations Center e o servidor do hub, deve-se usar a mesma senha para incluir o certificado do servidor do hub no arquivo de armazenamento confiável. Se você não se lembrar dessa senha, poderá reconfigurá-la.

A figura a seguir ilustra os componentes para configurar SSL entre o Operations Center e o servidor do hub.

Sobre Esta Tarefa

Este procedimento fornece etapas para implementar comunicações seguras usando certificados autoassinados.

Procedimento

Para configurar a comunicação de SSL usando certificados autoassinados, conclua as etapas a seguir.

1. Especifique o certificado `cert256.arm` como o certificado padrão no arquivo do banco de dados de chaves do servidor do hub:
   a. Emita o comando a seguir a partir do diretório de instâncias do servidor do hub:
      ```
      gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
           -label "TSM Server SelfSigned SHA Key"
      ```
   b. Reinicie o servidor do hub para que possa receber as mudanças para o arquivo do banco de dados de chave.
   c. Verifique se o certificado `cert256.arm` está configurado como o padrão. Emita o seguinte comando:
      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```
2. Pare o servidor da web Operations Center.
3. Abra a linha de comandos do sistema operacional no sistema em que o Operations Center está instalado e mude para o diretório a seguir:
   - AIX Linux *installation_dir*`/ui/jre/bin`
   - Windows *installation_dir*`\ui\jre\bin`

   Em que *installation_dir* representa o diretório no qual o Operations Center está instalado.
4. Abra a janela IBM Key Management emitindo o seguinte comando:
   ```
   ikeyman
   ```
5. Clique em **Arquivo do Banco de Dados de Chave** > **Abrir**.
6. Clique em **Procurar** e acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:
   - AIX Linux *installation_dir*`/ui/Liberty/usr/servers/guiServer`
   - Windows *installation_dir*`\ui\Liberty\usr\servers\guiServer`
7. No diretório `guiServer`, selecione o arquivo `gui-truststore.jks`.
8. Clique em **Abrir** e clique em **OK**.
9. Insira a senha para o arquivo de armazenamento confiável e clique em **OK**.
10. Na área Conteúdo do banco de dados de chaves da janela IBM Key Management, clique na seta e selecione **Certificados do assinante** da lista. Clique em **Incluir**.
11. Na janela Abrir, clique em **Procurar** e acesse o diretório de instância do servidor do hub:
    - AIX Linux `/opt/tivoli/tsm/server/bin`
    - Windows `c:\Program Files\Tivoli\TSM\server1`

    O diretório contém o `cert256.arm` certificado.

    Se não for possível acessar o diretório de instância do servidor do hub a partir da janela Abrir, conclua as etapas a seguir:
    a. Use o FTP ou outro método de transferência de arquivos para copiar os arquivos `cert256.arm` do servidor do hub para o seguinte diretório no computador em que o Operations Center está instalado:
       - AIX Linux *installation_dir*`/ui/Liberty/usr/servers/guiServer`

- Windows *installation_dir*\ui\Liberty\usr\servers\guiServer

b. Na janela Abrir, acesse o diretório guiServer.

12. Selecione o certificado cert256.arm como o certificado SSL.
13. Clique em **Abrir** e clique em **OK**.
14. Insira um rótulo para o certificado. Por exemplo, insira o nome do servidor do hub.
15. Clique em **OK**. O certificado SSL do servidor do hub é incluído no arquivo de armazenamento confiável e o rótulo é exibido na área Conteúdo do banco de dados de chaves da janela IBM Key Management.
16. Feche a janela IBM Key Management.
17. Inicie o servidor da web Operations Center. Ao conectar-se ao Operations Center pela primeira vez, você será solicitado a identificar o endereço IP ou o nome da rede do servidor do hub, além do número da porta para comunicação com o servidor do hub. Se a opção do servidor ADMINONCLIENTPORT estiver ativada para o servidor IBM Spectrum Protect, insira o número da porta que é especificado pela opção do servidor TCPADMINPORT. Se a opção do servidor ADMINONCLIENTPORT não estiver ativada, insira o número da porta especificado pela opção do servidor TCPPORT.

Tarefas relacionadas:

"Iniciando e parando o servidor da web" na página 109

Registrando a licença do produto

Para registrar sua licença para o produto IBM Spectrum Protect, use o comando **REGISTER LICENSE**.

Sobre Esta Tarefa

As licenças são armazenadas em arquivos de certificado de inscrição, que contêm informações sobre licença para o produto. Os arquivos de certificado de inscrição estão na mídia de instalação e são colocados no servidor durante a instalação. Ao registrar o produto, as licenças são armazenadas em um arquivo NODELOCK no diretório atual.

Procedimento

Registre uma licença especificando o nome do arquivo de certificado de inscrição que contém a licença. Para usar o construtor de comando do Operations Center para essa tarefa, conclua as etapas a seguir.

1. Abra o Operations Center.
2. Abra o construtor de comando do Operations Center, passando o mouse sobre o ícone de configurações e clicando em **Construtor de comando**.
3. Emita o comando **REGISTER LICENSE**. Por exemplo, para registrar uma licença do IBM Spectrum Protect base, emita o seguinte comando:

```
register license file=tsmbasic.lic
```

O que Fazer Depois

Salve a mídia de instalação que contém seus arquivos de certificado de inscrição. Pode ser necessário registrar sua licença novamente se, por exemplo, ocorrer uma das seguintes condições:

- O servidor foi movido para um computador diferente.
- O arquivo NODELOCK está corrompido. O servidor armazena informações sobre licença no arquivo NODELOCK, que está no diretório a partir do qual o servidor é iniciado.
- Linux Se você mudar o chip do processador associado ao servidor no qual o servidor está instalado.

Referências relacionadas:

REGISTER LICENSE (Registrar uma Nova Licença)

Configurando a deduplicação de dados

Crie um conjunto de armazenamentos de contêiner de diretório e pelo menos um diretório para usar a deduplicação de dados sequenciais.

Antes de Iniciar

Use as informações de diretório do conjunto de armazenamentos registradas no Capítulo 4, “Planilhas de planejamento”, na página 13 para essa tarefa.

Procedimento

1. Abra o Operations Center.
2. Na barra de menus do Operations Center, passe o mouse sobre **Armazenamento**.
3. Na lista exibida, clique em **Conjuntos de armazenamentos**.
4. Clique no botão **+Conjuntos de armazenamentos**.
5. Conclua as etapas no assistente Incluir conjunto de armazenamentos:
   - Para usar a deduplicação de dados sequenciais, selecione um conjunto de armazenamentos de **Diretório** no armazenamento baseado em contêiner.
   - Ao configurar diretórios para o conjunto de armazenamentos de contêiner de diretório, especifique os caminhos de diretório criados para armazenamento durante a configuração de sistema.
6. Após configurar o novo conjunto de armazenamentos de contêiner de diretório, clique em **Fechar e visualizar políticas** para atualizar a classe de gerenciamento e comece a usar o conjunto de armazenamentos.

Definindo regras de retenção de dados para seus negócios

Após criar um conjunto de armazenamentos de contêiner de diretório para deduplicação de dados, atualize a política do servidor padrão para usar o novo conjunto de armazenamentos. O assistente Incluir conjunto de armazenamentos abre a página Serviços no Operations Center para concluir esta tarefa.

Procedimento

1. Na página Serviços do Operations Center, selecione o domínio STANDARD e clique em **Detalhes**.
2. Na página Resumo do domínio de política, clique na guia **Conjuntos de políticas**. A página Conjuntos de políticas indica o nome do conjunto de políticas ativas e lista todas as classes de gerenciamento para esse conjunto de políticas.
3. Clique na alternância **Configurar** e faça as seguintes mudanças:

- Mude o destino de backup para a classe de gerenciamento STANDARD para o conjunto de armazenamentos de contêiner de diretório.
- Mude o valor para a coluna Backups para **Sem limite**.
- Mude o período de retenção. Configure a coluna Manter Backups Extras para 30 dias ou mais, dependendo de suas necessidades de negócios.

4. Salve suas mudanças e clique na alternância **Configurar** novamente de forma que o conjunto de políticas não seja mais editável.
5. Ative o conjunto de políticas clicando em **Ativar**.

Tarefas relacionadas:

"Especificando regras para backup e arquivamento de dados de cliente" na página 115

Definindo planejamentos para atividades de manutenção de servidor

Crie planejamentos para cada operação de manutenção de servidor usando o comando **DEFINE SCHEDULE** no construtor de comando do Operations Center.

Sobre Esta Tarefa

Planeje operações de manutenção do servidor para serem executadas após as operações de backup de cliente. É possível controlar a sincronização de planejamentos configurando o horário de início em conjunto com o tempo de duração de cada operação.

O exemplo a seguir mostra como você pode planejar processos de manutenção do servidor em combinação com o planejamento de backup de cliente para uma solução de disco multisite.

Operação	Planejamento
Backup de cliente	Inicia às 22h.
Replicação de nó	Inicia às 8h ou 10 horas após o início do backup de cliente.
Processamento para arquivos do banco de dados e de recuperação de desastre	• O backup de banco de dados começa às 11h ou 13 horas após o início do backup de cliente. Este processo é executado até a conclusão. • O backup de informações de configuração do dispositivo e do histórico do volume começa às 17h ou 6 horas após o início do backup de banco de dados. • A exclusão do histórico do volume começa às 20h, ou 9 horas após o início do backup de banco de dados.
Expiração de inventário	Inicia às 12h ou 14 após o início da janela de backup de cliente. Este processo é executado até a conclusão.

Procedimento

Depois de configurar a classe de dispositivo para as operações de backup de banco de dados, crie planejamentos para backup de banco de dados e outras operações de manutenção necessárias usando o comando **DEFINE SCHEDULE**. Dependendo do tamanho de seu ambiente, pode ser necessário ajustar os horários de início para cada planejamento no exemplo.

1. Defina uma classe de dispositivo para as operações de backup. Por exemplo, use o comando **DEFINE DEVCLASS** para criar uma classe de dispositivo chamada DBBACK_FILEDEV:

```
define devclass dbback_filedev devtype=file
  directory=db_backup_directories
```

em que *db_backup_directories* é uma lista dos diretórios que você criou para o backup de banco de dados.

AIX Linux Por exemplo, se você tem quatro diretórios para backup de banco de dados, iniciando com `/tsminst1/TSMbkup00`, emita o comando a seguir:

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

Windows Por exemplo, se você tiver quatro diretórios para backups de banco de dados, iniciando com `C:\tsminst1\TSMbkup00`, emita o comando a seguir:

```
define devclass dbback_filedev devtype=file
  directory="c:\tsminst1\TSMbkup00,
  c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,
  c:\tsminst1\TSMbkup03"
```

2. Configure a classe de dispositivo para operações de backup de banco de dados automáticas. Use o comando **SET DBRECOVERY** para especificar a classe de dispositivo criada na etapa anterior. Por exemplo, se a classe de dispositivo for dbback_filedev, emita o comando a seguir:

   ```
   set dbrecovery dbback_filedev
   ```

3. Crie planejamentos para as operações de manutenção, usando o comando **DEFINE SCHEDULE**. Consulte a tabela a seguir para as operações necessárias com exemplos dos comandos.

   Dica: Você cria o planejamento para replicação separadamente em uma etapa posterior, ao usar o Operations Center para configurar a replicação.

Operação	Exemplo de comando
Faça backup do banco de dados.	Crie um planejamento para executar o comando **BACKUP DB**. Se você estiver configurando um sistema pequeno, configure o parâmetro **COMPRESS** para `YES`. Por exemplo, em um sistema pequeno, emita o comando a seguir para criar um planejamento de backup que usa a nova classe de dispositivo: `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
Faça backup das informações de configuração do dispositivo.	Crie um planejamento para executar o comando **BACKUP DEVCONFIG**: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Faça backup do histórico do volume.	Crie um planejamento para executar o comando **BACKUP VOLHISTORY**: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes`

Operação	Exemplo de comando
Remova versões mais antigas dos backups de banco de dados que não sejam mais necessárias.	Crie um planejamento para executar o comando **DELETE VOLHISTORY**: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
Remova objetos que excedem sua retenção permitida.	Crie um planejamento para executar o comando **EXPIRE INVENTORY**. Configure o parâmetro **RESOURCE** com base no tamanho do sistema que está sendo configurado: • Sistemas pequenos: 10 • Sistemas médios: 30 • Sistemas grandes: 40 Por exemplo, em um sistema de tamanho médio, emita o comando a seguir para criar um planejamento denominado EXPINVENTORY: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

O que Fazer Depois

Depois de criar planejamentos para tarefas de manutenção de servidor, é possível visualizá-los no Operations Center concluindo as etapas a seguir:

1. Na barra de menus do Operations Center, passe o mouse sobre **Servidores**.
2. Clique em **Manutenção**.

Referências relacionadas:

DEFINE SCHEDULE (Definir um planejamento de um comando administrativo)

Definindo planejamentos de cliente

Use o Operations Center para criar planejamentos para operações do cliente.

Procedimento

1. Na barra de menus do Operations Center, passe o mouse sobre **Clientes**.
2. Clique em **Planejamentos**.
3. Clique em **+Schedule**.
4. Conclua as etapas no assistente Criar planejamento. Configure planejamentos de backup de cliente para iniciar às 22h, com base nas atividades de manutenção de servidor planejadas em “Definindo planejamentos para atividades de manutenção de servidor” na página 66.

Capítulo 10. Instalando e configurando clientes de backup-archive

Após a configuração bem-sucedida do sistema do servidor IBM Spectrum Protect, instale e configure o software cliente para iniciar o backup de dados.

Procedimento

Para instalar o cliente de backup-archive, siga as instruções de instalação para seu sistema operacional.

- Instale deus clientes de archive de backup do UNIX e do Linux
- Instalando o cliente Windows pela primeira vez

O que Fazer Depois

Registre e designe seus clientes a planejamentos.

Registrando e designando clientes a planejamentos

Inclua e registre seus clientes por meio do Operations Center usando o assistente Incluir cliente.

Antes de Iniciar

Determine se o cliente requer um ID do usuário administrativo com autoridade do proprietário cliente no nó cliente. Para determinar quais clientes requerem um ID do usuário administrativo, consulte a nota técnica 7048963.

Restrição: Para alguns tipos de clientes, o nome do nó cliente e o ID do usuário administrativo devem corresponder. Não é possível autenticar esses clientes usando o método de autenticação Lightweight Directory Access Protocol que foi introduzido na V7.1.7. Para obter detalhes sobre esse método de autenticação, às vezes referido como modo integrado, consulte Autenticando usuários usando um banco de dados do Active Directory.

Procedimento

Para registrar um cliente, conclua uma das seguintes ações.

- Se o cliente requerer um ID do usuário administrativo, registre o cliente usando o comando **REGISTER NODE** e especifique o parâmetro **USERID**:

  ```
  register node node_name password userid=node_name
  ```

  em que *node_name* especifica o nome do nó e *password* especifica a senha do nó. Para obter detalhes, consulte a seção Registrar um Nó.
- Se o cliente não requerer um ID de usuário administrativo, registre o cliente usando o assistente Incluir Cliente do Operations Center. Execute as etapas a seguir:
  1. Na barra de menus do Operations Center, clique em **Clientes**.
  2. Na tabela Clientes, clique em **+ Cliente**.
  3. Conclua as etapas no assistente Incluir cliente:

a. Especifique se os dados redundantes podem ser eliminados no cliente e no servidor. Na área de deduplicação de dados do lado do cliente, selecione a caixa de seleção **Ativar**.
b. Na janela Configuração, copie os valores das opções **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** e **DEDUPLICATION**.

   Dica: Registre os valores da opção e mantenha-os em um local seguro. Após concluir o registro do cliente e instalar o software no nó cliente, use os valores para configurar o cliente.
c. Siga as instruções no assistente para especificar o domínio de política, planejamento e conjunto de opções.
d. Configure como os riscos são exibidos para o cliente, especificando a configuração em risco.
e. Clique em **Incluir cliente**.

Instalando o serviço de gerenciamento de clientes

Instale o serviço de gerenciamento de clientes para clientes de backup-archive que são executados nos sistemas operacionais Linux e Windows. O serviço de gerenciamento de cliente coleta informações de diagnóstico sobre clientes de backup-archive e torna as informações disponíveis para o Operations Center para capacidade de monitoramento básico.

Procedimento

Instale o serviço de gerenciamento de clientes no mesmo computador que o cliente de backup-archive, concluindo as etapas a seguir:

1. Faça download do pacote de instalação para o serviço de gerenciamento de clientes de um site de download da IBM, como IBM Passport Advantage® ou IBM Fix Central. Procure por um nome do arquivo que seja semelhante a `<version>-IBM_Spectrum_Protect-CMS-operating_system.bin`.
2. Crie um diretório no sistema do cliente que deseja gerenciar e copie o pacote de instalação nesse diretório.
3. Extraia o conteúdo do arquivo do pacote de instalação.
4. Execute o arquivo de lote de instalação a partir do diretório onde foram extraídos os arquivos de instalação e associados. Este é o diretório criado na etapa 2.
5. Para instalar o serviço de gerenciamento de clientes, siga as instruções no assistente do IBM Installation Manager. Se o IBM Installation Manager ainda não estiver instalado no sistema do cliente, deve-se selecionar o IBM Installation Manager e o IBM Spectrum Protect Client Management Services.

Tarefas relacionadas:

Configurando o serviço de gerenciamento de cliente para instalações do cliente customizado

Verificando que o serviço de gerenciamento de clientes está instalado corretamente

Antes de usar o serviço de gerenciamento de clientes para coletar informações de diagnóstico sobre um cliente de backup-archive, é possível verificar se o serviço de gerenciamento de clientes está instalado e configurado corretamente.

Procedimento

Na linha de comandos do sistema do cliente, execute os seguintes comandos para visualizar a configuração do client management service:

- Nos sistemas do cliente Linux, emita o seguinte comando:

  ```
  client_install_dir/cms/bin/CmsConfig.sh list
  ```

  em que *client_install_dir* é o diretório no qual o cliente de backup-archive está instalado. Por exemplo, com a instalação do cliente padrão, emita o comando a seguir:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  A saída é semelhante ao seguinte texto:

  ```
  Listando a configuração CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Capacidades: [LOG_QUERY]
      Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Arquivo de Log: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Arquivo de Log: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

- Nos sistemas do cliente Windows, emita o seguinte comando:

  ```
  client_install_dir\cms\bin\CmsConfig.bat list
  ```

  em que *client_install_dir* é o diretório no qual o cliente de backup-archive está instalado. Por exemplo, com a instalação do cliente padrão, emita o comando a seguir:

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  A saída é semelhante ao seguinte texto:

  ```
  Listando a configuração CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Capacidades: [LOG_QUERY]
      Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Se o client management service estiver instalado e configurado corretamente, a saída exibirá o local do arquivo de log de erro.
O texto de saída é extraído do arquivo de configuração a seguir:

- Nos sistemas do cliente Linux:

  ```
  client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
  ```

- Nos sistemas do cliente Windows:

client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml

Se a saída não contiver nenhuma entrada, deve-se configurar o arquivo `client-configuration.xml`. Para obter instruções sobre como configurar este arquivo, consulte Configurando o serviço de gerenciamento de cliente para instalações do cliente customizado. É possível usar o comando **CmsConfig verify** para verificar que a definição de nó está corretamente criada no arquivo `client-configuration.xml`.

Configurando o Operations Center para usar o serviço de gerenciamento de clientes

Se você não usou a configuração padrão para o serviço de gerenciamento de clientes, deve-se configurar o Operations Center para acessar o serviço de gerenciamento de clientes.

Antes de Iniciar

Certifique-se de que o serviço de gerenciamento de clientes esteja instalado e iniciado no sistema do cliente. Verifique se a configuração padrão é usada. A configuração padrão não será usada se uma das condições a seguir for atendida:

- O serviço de gerenciamento de clientes não usa o número da porta padrão, 9028.
- O cliente de backup-archive não é acessado pelo mesmo endereço IP do sistema do cliente no qual o cliente de backup-archive está instalado. Por exemplo, um endereço IP diferente pode ser usado nas situações a seguir:
  - O sistema de computador possui duas placas de rede. O cliente de backup-archive está configurado para se comunicar em uma rede, enquanto o serviço de gerenciamento de clientes se comunica na outra rede.
  - O sistema do cliente está configurado com o Protocolo de Configuração de Host Dinâmico (DHCP). Como resultado, o sistema do cliente é designado dinamicamente a um endereço IP, que é salvo no servidor durante a operação do cliente de backup-archive anterior. Quando o sistema do cliente é reiniciado, esse sistema poderá ser designado a um endereço IP diferente. Para assegurar que o Operations Center sempre possa localizar o sistema do cliente, especifique um nome de domínio completo.

Procedimento

Para configurar o Operations Center para usar o serviço de gerenciamento de clientes, conclua as etapas a seguir:

1. Na página Clientes do Operations Center, selecione o cliente.
2. Clique em **Detalhes** > **Propriedades**.
3. No campo URL de diagnósticos remotos na seção geral, especifique a URL para o serviço de gerenciamento de clientes no sistema do cliente. O endereço deve iniciar com `https`. A tabela a seguir mostra exemplos da URL de diagnósticos remota.

Tipo de URL	Exemplo
Com o nome do host DNS e porta padrão 9028	`https://server.example.com`
Com o nome do host DNS e porta não padrão	`https://server.example.com:1599`
Com o endereço IP e porta não padrão	`https://192.0.2.0:1599`

4. Clique em **Salvar**.

O que Fazer Depois

É possível acessar informações de diagnóstico do cliente, como arquivos de log do cliente, a partir da guia **Diagnósticos** no Operations Center.

Capítulo 11. Configurando o segundo servidor

Após concluir a configuração do primeiro servidor em seu sistema, configure o segundo servidor.

Procedimento

Conclua as instrução nas seções a seguir:

1. Configure um segundo servidor que seja igual ao primeiro servidor, completando as instruções nas seções a seguir:
   a. Capítulo 7, "Configurando o sistema", na página 37
   b. Capítulo 8, "Instalando o servidor e o Operations Center", na página 53

      Apenas um servidor na solução de disco multisite é configurado como o servidor do hub, portanto, você não precisa instalar o Operations Center no segundo servidor. Quando você selecionar os pacotes de instalação para instalar no segundo servidor, não selecione o Operations Center.
   c. Capítulo 9, "Configurando o servidor e o Operations Center", na página 57

      Ignore as tarefas para configurar o Operations Center.
   d. Capítulo 10, "Instalando e configurando clientes de backup-archive", na página 69
2. "Configurando comunicações de SSL entre o servidor do hub e um servidor spoke"
3. "Incluindo o segundo servidor como um spoke" na página 77
4. "Ativando a replicação" na página 77

Configurando comunicações de SSL entre o servidor do hub e um servidor spoke

Para uma comunicação segura entre o servidor do hub e um servidor spoke usando o protocolo de Segurança da Camada de Transporte (TLS), você deve definir o certificado do servidor spoke para o servidor do hub.

Sobre Esta Tarefa

O servidor hub recebe informações de status e alerta do servidor spoke e mostra essas informações no Operations Center. Para receber as informações de status e alerta do servidor spoke, o certificado do servidor spoke deve ser incluído no arquivo de armazenamento confiável do servidor do hub. Você deve também configurar o Operations Center para monitorar o servidor spoke.

Para ativar outras funções do Operations Center, como a implementação automática de atualizações de cliente, o certificado do servidor do hub deve ser incluído no arquivo de armazenamento confiável do servidor spoke.

Procedimento

1. Conclua as seguintes etapas para definir o certificado do servidor spoke para o servidor do hub:
   a. No servidor spoke, vá para o diretório da instância do servidor spoke.

b. Especifique o certificado `cert256.arm` requerido como o certificado padrão no arquivo do banco de dados de chave do servidor spoke. Emita o seguinte comando:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
 -label "TSM Server SelfSigned SHA Key"
```

c. Verifique os certificados no arquivo do banco de dados de chave do servidor spoke. Emita o seguinte comando:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

d. Transfira com segurança o arquivo `cert256.arm` do servidor spoke para o servidor do hub.

e. No servidor do hub, vá para o diretório da instância do servidor do hub.

f. Defina o certificado do servidor spoke para o servidor do hub. Emita o comando a seguir a partir do diretório de instância do servidor do hub, em que *spoke_servername* é o nome do servidor spoke e *spoke_cert256.arm* é o nome do arquivo do certificado do servidor spoke:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
 -label spoke_servername -file spoke_cert256.arm
```

2. Conclua as seguintes etapas para definir o certificado do servidor do hub para o servidor spoke:

a. No servidor do hub, vá para o diretório da instância do servidor do hub.

b. Especifique o certificado `cert256.arm` necessário como certificado padrão no arquivo do banco de dados de chave do servidor do hub. Emita o seguinte comando:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
 -label "TSM Server SelfSigned SHA Key"
```

c. Verifique os certificados no arquivo do banco de dados de chave do servidor spoke. Emita o seguinte comando:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

d. Transfira o arquivo `cert256.arm` de maneira segura do servidor do hub para o servidor spoke.

e. No servidor spoke, vá para o diretório da instância do servidor spoke.

f. Defina o certificado do servidor do hub para o servidor spoke. Emita o comando a seguir a partir do diretório de instância do servidor spoke, em que *hub_servername* é o nome do servidor do hub e *hub_cert256.arm* é o nome do arquivo do certificado do servidor do hub:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
 -label hub_servername -file hub_cert256.arm
```

3. Reinicie o servidor do hub e o servidor spoke.

4. Conclua as etapas a seguir para definir o servidor spoke para o servidor do hub e o servidor do hub para o servidor spoke.

a. Emita os seguintes comandos no servidor do hub e no servidor spoke:

```
SET SERVERPASSWORD server_password
SET SERVERHLADDRESS ip_address
SET SERVERLLADDRESS tcp_port
```

b. No servidor do hub, emita o comando **DEFINE SERVER**, de acordo com o exemplo a seguir:

```
DEFINE SERVER spoke_servername HLA=spoke_address
 LLA=spoke_SSLTCPADMINPort SERVERPA=spoke_serverpassword
```

c. No servidor spoke, emita o comando **DEFINE SERVER**, de acordo com o exemplo a seguir:

```
DEFINE SERVER hub_servername HLA=hub_address
 LLA=hub_SSLTCPADMINPort SERVERPA=hub_serverpassword
```

Dica: Por padrão, a comunicação do servidor é criptografada, exceto quaando o servidor envia ou recebe dados do objeto. Dados do objeto são enviados e recebidos usando TCP/IP. Escolhendo não criptografar os dados do objeto, o desempenho do servidor é semelhante à comunicação sobre uma sessão TCP/IP e a sessão é segura. Para criptografar toda a comunicação com o servidor especificado, mesmo quando o servidor estiver enviando ou recebendo dados do objeto, especifique o parâmetro SSL=YES no comando **DEFINE SERVER**.

5. Conclua as seguintes etapas para configurar o Operations Center para monitorar o servidor spoke:
   a. Na barra de menus do Operations Center, clique em **Servidores**. O servidor spoke possui um status de "Não monitorado." Esse status significa que, embora este servidor tenha sido definido para o servidor do hub usando o comando **DEFINE SERVER**, o servidor ainda não está configurado como spoke.
   b. Clique no servidor spoke para destacar o item e, em seguida, clique em **Monitorar Spoke**.

Referências relacionadas:

DEFINE SERVER (Definir um Servidor para Comunicações Servidor-para-Servidor)

QUERY OPTION (Consultar opções do servidor)

Incluindo o segundo servidor como um spoke

Após configurar os dois servidores em seu ambiente, inclua o segundo servidor como um spoke no servidor do hub.

Procedimento

1. Abra o Operations Center.
2. Na barra de menus Operations Center, clique em **Servidores**.
3. Conclua uma das etapas a seguir:
   - Clique no servidor para destacá-lo e na barra de menus da tabela, clique em **Monitorar Spoke**.
   - Se o servidor que você deseja incluir não for mostrado na tabela, clique em **+Spoke**.
4. Conclua as etapas no assistente de configuração spoke.

Ativando a replicação

Para proteger seus dados, ative a replicação de nó, além de proteger seus conjuntos de armazenamentos.

Procedimento

Para ativar a replicação de nó para todos os clientes que estão registrados no servidor de origem, conclua as etapas a seguir

1. Abra o Operations Center.
2. Na barra de menus do Operations Center, passe o mouse sobre **Armazenamento** e clique em **Replicação**.
3. Na página **Replicação**, clique em **+ Par de servidores**.
4. Conclua as etapas no assistente Incluir par do servidor:

- Configure o servidor de origem como o primeiro servidor que você configurou para a solução de disco multisite. O servidor de destino é o segundo servidor.
- Configure o planejamento de replicação de nó para iniciar 10 horas depois da janela de backup do cliente, com base nas atividades de manutenção do servidor que você planejou em "Definindo planejamentos para atividades de manutenção de servidor" na página 66.
- O assistente configura planejamentos de proteção do conjunto de armazenamentos para você, com base na quantidade de dados que estão sendo protegidos e em quando a replicação de cliente é planejada.

O que Fazer Depois

Se você planeja configurar a replicação mútua entre os dois sites, execute o assistente Incluir par de servidores novamente e configure o segundo servidor como a origem e o primeiro servidor como o destino.

Capítulo 12. Concluindo a implementação

Após a solução IBM Spectrum Protect estar configurada e em execução, teste as operações de backup e configure o monitoramento para assegurar que tudo seja executado corretamente.

Procedimento

1. Teste as operações de backup para verificar se seus dados estão protegidos como você espera.
   a. Na página Clientes do Operations Center, selecione os clientes do qual deseja fazer backup e clique em **Fazer backup**.
   b. Na página Servidores do Operations Center, selecione o servidor para o qual deseja fazer backup do banco de dados. Clique em **Fazer backup** e siga as instruções na janela Fazer backup do banco de dados.
   c. Verifique se as operações de backup foram concluídas com sucesso sem nenhum aviso ou mensagens de erro.

      Dica: Como alternativa, é possível usar a GUI do cliente de backup-archive para fazer backup de dados do cliente e é possível fazer backup do banco de dados do servidor emitindo o comando **BACKUP DB** de uma linha de comandos administrativa.
2. Configure o monitoramento para sua solução seguindo as instruções em Parte 3, “Monitorando uma solução de disco multisite”, na página 81.

Parte 3. Monitorando uma solução de disco multisite

Após implementar uma solução de disco multisite com o IBM Spectrum Protect, monitore a solução para assegurar a operação correta. Ao monitorar a solução diária e periodicamente, é possível identificar problemas existentes e em potencial. As informações reunidas podem ser usadas para resolver problemas e otimizar o desempenho do sistema.

Sobre Esta Tarefa

A maneira preferencial de monitorar uma solução é usar o Operations Center, que fornece um status do sistema geral e detalhado em uma interface gráfica com o usuário. Além disso, é possível configurar o Operations Center para gerar um relatório de email diário que resume o status do sistema.

El alguns casos, talvez você queira usar ferramentas de monitoramento avançado para concluir tarefas específicas de monitoramento ou de resolução de problemas.

Dica: Se você planeja diagnosticar problemas com clientes de backup-archive nos sistemas operacionais Linux ou Windows, instale os serviços de gerenciamento do cliente do IBM Spectrum Protect em cada computador em que um cliente de backup-archive estiver instalado. Dessa forma, é possível assegurar que o botão **Diagnosticar** esteja disponível no Operations Center para diagnosticar problemas com clientes de backup-archive. Para instalar o serviço de gerenciamento de clientes, siga as instruções em "Instalando o serviço de gerenciamento de clientes" na página 70.

Procedimento

1. Concluir tarefas de monitoramento diárias. Para obter instruções, consulte Capítulo 13, "Lista de verificação de monitoramento diária", na página 83.
2. Concluir tarefas de monitoramento periódicas. Para obter instruções, consulte Capítulo 14, "Lista de verificação de monitoramento periódica", na página 93.
3. Para verificar se a solução do IBM Spectrum Protect está em conformidade com os requisitos de licença, siga as instruções em Capítulo 15, "Verificando a conformidade da licença", na página 101.
4. Para configurar o Operations Center para gerar relatórios de status de e-mail, veja Capítulo 16, "Rastreando o status do sistema usando relatórios de e-mail", na página 103

O que Fazer Depois

Resolva quaisquer problemas que forem detectados. Para resolver um problema, alterando a configuração de sua solução, siga as instruções em Parte 4, "Gerenciando operações para uma solução de disco multisite", na página 105. Os recursos a seguir também estão disponíveis:

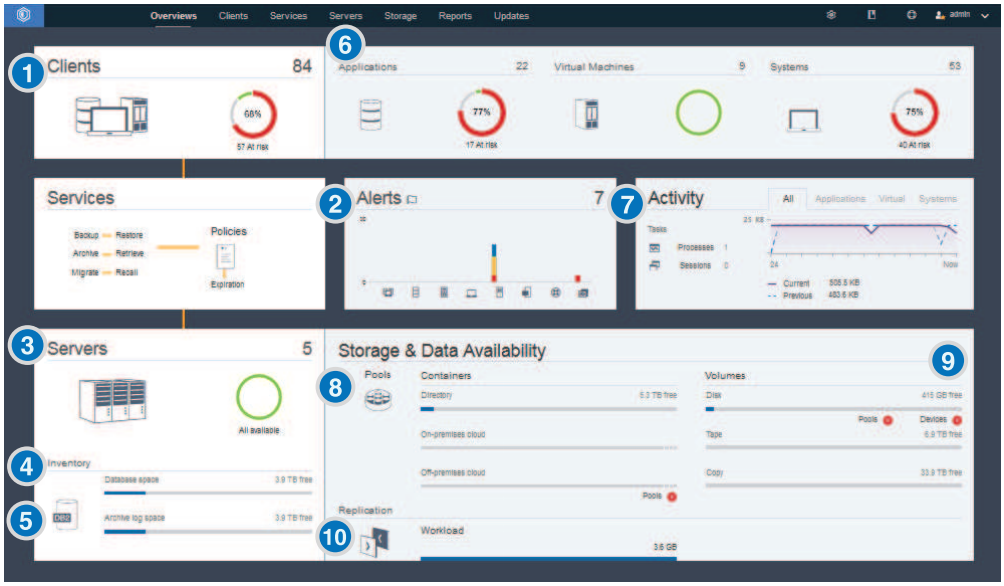
- Para resolver problemas de desempenho, consulte Desempenho.
- Para resolver outros tipos de problemas, consulte Resolução de problemas.

Capítulo 13. Lista de verificação de monitoramento diária

Para assegurar que você esteja concluindo as tarefas diárias de monitoramento para sua solução IBM Spectrum Protect, revise a lista de verificação diária de monitoramento.

Conclua as tarefas de monitoramento diárias a partir da página Visão geral do Operations Center. É possível acessar a página Visão geral abrindo o Operations Center e clicando em **Visões gerais**.

A figura a seguir mostra o local para conclusão de cada tarefa.



Dica: Para executar comandos administrativos para tarefas de monitoramento avançado, use o construtor de comando do Operations Center. O construtor de comando fornece uma função de digitação antecipada para orientá-lo conforme você insere comandos. Para abrir o construtor de comando, acesse a página Visão geral do Operations Center. Na barra de menus, passe o mouse sobre o ícone de configurações e clique em **Construtor de comando**.

A tabela a seguir lista as tarefas de monitoramento de diárias e fornece instruções para concluir cada tarefa.

Tabela 15. Tarefas de monitoramento diárias

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
Observe as notificações de segurança, que podem indicar um ataque de ransomware.	Se um ataque de ransomware em potencial for detectado no ambiente do IBM Spectrum Protect, uma mensagem de notificação de segurança será exibida no primeiro plano do Operations Center. Para obter mais informações, clique na mensagem para abrir a página Notificações de segurança.	Na página Notificações de segurança, é possível tomar as ações a seguir: • Visualizar detalhes de notificação por cliente. **Restrição:** As notificações estão disponíveis apenas para os clientes de backup e archive e os clientes do IBM Spectrum Protect for Virtual Environments. • Reconhecer uma notificação de segurança selecionando-a e clicando em **Reconhecer**. Quando você reconhece uma notificação de segurança, um visto é incluído na coluna Reconhecido da página Notificações de segurança para o cliente selecionado. O padrão pelo qual uma notificação é reconhecida é determinado por sua organização. Um visto pode significar que você investigou o problema e determinou que ele é um falso positivo. Ou pode significar que um problema existe e está sendo resolvido. • Designar uma notificação de segurança para um administrador selecionando a notificação de segurança e clicando em **Designar**. Para visualizar a designação, o administrador deve conectar-se ao Operations Center e clicar em **Visões gerais** > **Segurança**. Se você não tiver certeza de que o administrador monitora regularmente a página Notificações de segurança, notifique o administrador sobre a designação. • Se a notificação for um falso positivo, será possível selecionar a notificação de segurança e clicar em **Reconfigurar**. A notificação de segurança é excluída. Os dados históricos que são usados para comparações de linha de base com a operação de backup mais recente são excluídos. Uma nova linha de base é calculada daí em diante.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
1 Determine se os clientes correm risco de ficarem desprotegidos devido a operações de backup com falha ou ausentes.	Para verificar se os clientes estão em risco, na área de Clientes, procure uma notificação **Em risco**. Para visualizar detalhes, clique na área Clientes. **Atenção:** Se a porcentagem **Em risco** for muito maior do que o normal, isso poderá indicar um ataque de ransomware. Um ataque de ransomware pode fazer com que as operações de backup falhem, colocando os clientes em risco. Por exemplo, se a porcentagem de clientes em risco normalmente estiver entre 5% e 10%, mas aumentar para 40% ou 50%, investigue a causa. Se você instalou o serviço de gerenciamento de clientes em um cliente de backup-archive, será possível visualizar e analisar os logs de erro e de planejamento, concluindo as etapas a seguir: 1. Na tabela Clientes, selecione o cliente e clique em **Detalhes**. 2. Para diagnosticar um problema, clique em **Diagnóstico**.	Para clientes que não têm o serviço de gerenciamento de clientes instalado, acesse o sistema do cliente para revisar os logs de erro do cliente.
2 Determine se os erros relacionados ao cliente ou ao servidor requerem atenção.	Para determinar a gravidade de qualquer um dos alertas relatados, na área Alertas, passe o mouse sobre as colunas.	Para visualizar informações adicionais sobre alertas, conclua as etapas a seguir: 1. Clique na área Alertas. 2. Na tabela Alertas, selecione um alerta. 3. Na área de janela Log de atividades, revise as mensagens. A área de janela exibe mensagens relacionadas que foram emitidas antes e após o alerta selecionado ter ocorrido.
3 Determine se os servidores que são gerenciados pelo Operations Center estão disponíveis para fornecer serviços de proteção de dados para clientes.	1. Para verificar se os servidores estão em risco, na área Servidores, procure uma notificação **Indisponível**. 2. Para visualizar informações adicionais, clique na área Servidores. 3. Selecione um servidor na tabela Servidores e clique em **Detalhes**.	**Dica:** Se você detectar um problema que está relacionado às propriedades do servidor, atualize as propriedades do servidor: 1. Na tabela Servidores, selecione um servidor e clique em **Detalhes**. 2. Para atualizar propriedades do servidor, clique em **Propriedades**.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
4 Determine se há espaço suficiente disponível para o inventário do servidor, que consiste no banco de dados do servidor, no log ativo e no log de archive.	1. Clique na área Servidores. 2. Na coluna Status da tabela, visualize o status do servidor e resolva os problemas: • **Normal** Há espaço suficiente disponível para o banco de dados do servidor, o log ativo e o log de archive. • **Crítico** Não há espaço suficiente disponível para o banco de dados do servidor, o log ativo ou o log de archive. Deve-se incluir espaço imediatamente ou os serviços de proteção de dados que são fornecidos pelo servidor serão interrompidos. • **Aviso** O banco de dados do servidor, o log ativo ou o log de archive estão sem espaço. Se essa condição persistir, deve-se incluir espaço. • **Indisponível** O status não pode ser obtido. Certifique-se de que o servidor esteja em execução e que não haja problemas de rede. Este status também será mostrado se o ID de administrador de monitoramento estiver bloqueado ou, de outra forma, indisponível no servidor. Este ID é denominado IBM-OC-hub_server_name. • **Não monitorado** Os servidores não monitorados estão definidos para o servidor do hub, mas não estão configurados para gerenciamento pelo Operations Center. Para configurar um servidor não monitorado, selecione o servidor e clique em **Monitorar spoke**.	Também é possível procurar alertas relacionados na página Alertas. Para obter instruções adicionais sobre resolução de problemas, consulte Resolvendo Problemas do Servidor.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
5 Verifique as operações de backup de banco de dados do servidor.	Para determinar quando um servidor foi submetido a backup mais recentemente, conclua as etapas a seguir: 1. Clique na área Servidores. 2. Na tabela Servidores, revise a coluna Último backup de banco de dados.	Para obter informações mais detalhadas sobre as operações de backup, conclua as etapas a seguir: 1. Na tabela Servidores, selecione uma linha e clique em **Detalhes**. 2. Na área Backup do BD, passe o mouse sobre as marcas de seleção para revisar informações sobre operações de backup. Se um banco de dados não foi submetido a backup recentemente (por exemplo, nas últimas 24 horas), é possível iniciar uma operação de backup: 1. Na página Visão geral do Operations Center, clique na área Servidores. 2. Na tabela, selecione um servidor e clique em **Fazer backup**. Para determinar se o banco de dados do servidor está configurado para operações de backup automático, conclua as etapas a seguir: 1. Na barra de menus, passe o mouse sobre o ícone de configurações e clique em **Construtor de comando**. 2. Emita o comando **QUERY DB**: `query db f=d` 3. Na saída, revise o campo `Nome completo da classe de dispositivo`. Se uma classe de dispositivo for especificada, o servidor será configurado para backups de banco de dados automáticos.
6 Monitore outras tarefas de manutenção de servidor. As tarefas de manutenção de servidor podem incluir a execução de planejamentos de comandos administrativos, de scripts de manutenção e de comandos relacionados.	Para procurar informações sobre processos que falharam devido a problemas do servidor, conclua as etapas a seguir: 1. Clique em **Servidores** > **Manutenção**. 2. Para obter o histórico de duas semanas de um processo, visualize a coluna Histórico. 3. Para obter informações adicionais sobre um processo planejado, passe o mouse sobre a caixa de seleção que está associada ao processo.	Para obter informações adicionais sobre como monitorar processos e resolver problemas, consulte a ajuda online do Operations Center.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
7 Verifique se a quantidade de dados que foram enviados recentemente para e de servidores está dentro do intervalo esperado.	• Para obter uma visão geral de atividade nas últimas 24 horas, visualize a área Atividade. • Para comparar a atividade nas últimas 24 horas com a atividade nas 24 horas anteriores, revise os números nas áreas Atual e Anterior.	• Se foram enviados ao servidor mais dados do que o esperado, determine quais clientes estão fazendo backup de mais dados e investigue a causa. É possível que a deduplicação de dados do lado do cliente não esteja funcionando corretamente. **Atenção:** Se a quantidade de dados de backup é significativamente maior que o normal, isso pode indicar um ataque de ransomware. Quando o ransomware criptografa dados, o sistema detecta os dados como sendo mudados e tais dados mudados são submetidos a backup. Assim, volumes de backup se tornam maiores. Para determinar quais clientes são afetados, clique na guia **Aplicativos**, **Máquinas virtuais** ou **Sistemas**. • Se foram enviados ao servidor menos dados do que o esperado, investigue se as operações de backup do cliente continuam dentro do planejamento.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
8 Verifique se os conjuntos de armazenamentos estão disponíveis para fazer backup de dados de cliente.	1. Se os problemas forem indicados na área Armazenamento e Disponibilidade de dados, clique em **Conjuntos** para visualizar os detalhes: • Se o status **Crítico** for exibido, não há espaço suficiente disponível no conjunto de armazenamentos ou seu status de acesso está indisponível. **Atenção:** Se o status for crítico, investigue a causa: – Se a taxa de deduplicação de dados para um conjunto de armazenamentos cair significativamente, isso poderá indicar um ataque de ransomware. Durante um ataque de ransomware, os dados são criptografados e não podem ser deduplicados. Para verificar a taxa de deduplicação de dados, na tabela Conjuntos de Armazenamento, revise o valor na coluna % de Economia. – Se um conjunto de armazenamento inesperadamente torna-se 100% utilizado, isso pode indicar um ataque de ransomware. Para verificar a utilização, revise o valor na coluna Capacidade Utilizada. Passe o mouse sobre os valores para ver as porcentagens de espaço usado e livre. • Se o status **Aviso** for exibido, o conjunto de armazenamentos está sem espaço ou seu status de acesso é somente leitura. 2. Para visualizar o espaço usado, livre e total para seu conjunto de armazenamentos selecionado, passe o mouse sobre as entradas na coluna Capacidade utilizada.	Para visualizar a capacidade do conjunto de armazenamentos que foi usada nas últimas duas semanas, selecione uma linha na tabela Conjuntos de armazenamentos e clique em **Detalhes**.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
9 Verifique se há dispositivos de armazenamento disponíveis para operações de backup.	Na área Armazenamento e disponibilidade de dados, na seção Volumes, sob as barras de capacidade, revise o status que é suportado, ao lado de **Dispositivos**. Se um status **Crítico** ou **Aviso** for exibido para qualquer dispositivo, investigue o problema. Para visualizar detalhes, clique em **Dispositivos**.	Os dispositivos de disco podem ter um status crítico ou de aviso pelos seguintes motivos: • Para classes de dispositivo DISK, os volumes podem estar off-line ou ter um status de acesso somente leitura. A coluna Armazenamento em disco da tabela Dispositivos de disco mostra o estado dos volumes. • Para classes de dispositivo FILE que não são compartilhadas, os diretórios podem estar offline. Além disso, pode haver espaço livre insuficiente disponível para alocar volumes utilizáveis. A coluna Armazenamento em disco da tabela Dispositivos de disco mostra o estado dos diretórios. • Para classes de dispositivo FILE que são compartilhadas, as unidades podem ficar indisponíveis. Uma unidade estará indisponível se estiver off-line, tiver parado de responder ao servidor ou se seu caminho estiver off-line. Outras colunas da tabela Dispositivos de disco mostram o estado das unidades e caminhos.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
10 Monitorar processos de replicação de nó.	1. Para obter o status geral de processos de replicação de nó, visualize a área Replicação na página Visão geral do Operations Center. 2. Para visualizar informações sobre cada par de servidores replicados, clique na área Replicação. **Atenção:** Se você observar um aumento inesperado no número de falhas de replicação, isso poderá indicar um ataque de ransomware. Investigue a causa da falha. 3. Para visualizar a quantia de dados que foi replicada nas duas últimas semanas e a velocidade da replicação, selecione um par de servidores e clique em **Detalhes**. 4. Para visualizar informações de replicação para um cliente, na página Visão geral do Operations Center, clique em **Clientes**. Visualize as informações na coluna Carga de trabalho de replicação. **Atenção:** Se você vir um aumento drástico e inesperado na carga de trabalho de replicação, isso poderá indicar um ataque de ransomware. Investigue a causa do aumento da carga de trabalho.	Para monitoramento avançado, visualize informações sobre processos de replicação de nó em execução e encerrados usando comandos: 1. Na página de visão geral do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Cconstrutor de comando**. 2. Emita o comando **QUERY REPLICATION**. Para obter instruções, consulte QUERY REPLICATION (Consultar Processos de Replicação de Nó). Se a operação de replicação foi concluída com sucesso, o valor `Total de arquivos para replicação` corresponderá ao valor `Total de arquivos replicados`. Para exibir mensagens relacionadas a um processo de replicação de nó em um servidor de replicação de origem ou de destino, conclua as etapas a seguir: 1. Na página Visão geral do Operations Center, clique em **Servidores**. 2. Selecione o servidor de replicação de origem ou de destino e clique em **Detalhes**: • Para visualizar tarefas ativas, clique em **Tarefas ativas**, selecione a tarefa e verifique se o status **Em execução** é exibido. Para obter detalhes, visualize os logs de atividades relacionados. • Para visualizar tarefas concluídas, clique em **Tarefas concluídas**, selecione a tarefa e certifique-se de que o status **Concluído** seja exibido. Para obter detalhes, visualize os logs de atividades relacionados.

Tabela 15. Tarefas de monitoramento diárias (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e informações de resolução de problemas
11 Monitorar conjuntos de retenção.	Para obter o status geral dos conjuntos de retenção, visualize a área **Conjuntos de Retenção** na página Visão geral do Operations Center: • O campo **Concluído** especifica o número de conjuntos de retenção que foram criados no banco de dados do servidor e que são rastreados no inventário do servidor. • O campo **Concluído** especifica o número de conjuntos de retenção que possuem dados expirados. • O campo **Excluído** especifica o número de conjuntos de retenção que foram excluídos. Para visualizar ou modificar as regras de retenção, clique em **Serviços** > **Regras de retenção**.	Para obter mais informações sobre os conjuntos de retenção, clique na área **Conjuntos de retenção** para abrir a página Conjuntos de retenção. Para visualizar ou modificar as propriedades de conjuntos de retenção, dê um clique duplo em um conjunto de retenção. Para obter informações mais detalhadas, é possível executar comandos relacionados: 1. Na página de visão geral do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Cconstrutor de comando**. 2. Para determinar quais tarefas de criação de conjunto de retenção estão em execução, interrompidas ou concluídas, execute o comando **QUERY JOB**. Para obter instruções, consulte QUERY JOB (Consultar uma tarefa de criação do conjunto de retenção). 3. Para consultar regras de retenção, execute o comando **QUERY RETRULE**. Para obter instruções, consulte QUERY RETRULE (Consultar uma regra de retenção). 4. Para consultar conjuntos de retenção, execute o comando **QUERY RETSET**. Para obter instruções, consulte QUERY RETSET (Consultar um conjunto de retenção). 5. Para consultar o conteúdo de conjuntos de retenção, execute o comando **QUERY RETSETCONTENTS**. Para obter instruções, consulte QUERY RETSETCONTENTS (Consultar os conteúdos de um conjunto de retenção).

Capítulo 14. Lista de verificação de monitoramento periódica

Para ajudar a assegurar que sua solução funcione corretamente, conclua as tarefas na lista de verificação de monitoramento periódica. Planeje tarefas periódicas com frequência suficiente para que seja possível detectar possíveis problemas antes que eles se tornem problemáticos.

Dica: Para executar comandos administrativos para tarefas de monitoramento avançado, use o construtor de comando do Operations Center. O construtor de comando fornece uma função de digitação antecipada para orientá-lo conforme você insere comandos. Para abrir o construtor de comando, acesse a página Visão geral do Operations Center. Na barra de menus, passe ou mouse sobre o ícone de configurações  e clique em **Construtor de comando**.

Tabela 16. Tarefas de monitoramento periódicas

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Monitore o desempenho do sistema.	Determine o período de tempo necessário para operações de backup do cliente: 1. Na página Visão geral do Operations Center, clique em **Clientes**. Localize o servidor que está associado ao cliente. 2. Clique em **Servidores**. Selecione o servidor e clique em **Detalhes**. 3. Para visualizar a duração de tarefas concluídas nas últimas 24 horas, clique em **Tarefas concluídas**. 4. Para visualizar a duração de tarefas que foram concluídas mais de 24 horas atrás, use o comando **ACTLOG QUERY**. Siga as instruções em . 5. Se a duração de operações de backup do cliente estiver aumentando e as razões não forem claras, investigue a causa. Se você instalou o serviço de gerenciamento de clientes em um cliente de backup-archive, será possível diagnosticar problemas de desempenho para o cliente de backup-archive concluindo as etapas a seguir: 1. Na página Visão geral do Operations Center, clique em **Clientes**. 2. Selecione um cliente de backup-archive e clique em **Detalhes**. 3. Para recuperar logs do cliente, clique em **Diagnóstico**.	Para obter instruções sobre como reduzir o tempo gasto para o cliente fazer backup de dados para o servidor, consulte Resolvendo Problemas de Desempenho Comuns do Cliente. Procure gargalos de desempenho. Para obter instruções, consulte Identificando Gargalos de Desempenho. Para obter informações sobre como identificar e resolver outros problemas de desempenho, consulte Desempenho.

Tabela 16. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Determine a economia de disco fornecida pela deduplicação de dados.	1. Na página Visão geral do Operations Center, clique em **Conjuntos**. 2. Selecione um conjunto e clique em **Verificação rápida**. 3. Na área Deduplicação de dados, visualize a linha Espaço salvo.	Para monitoramento avançado, para obter estatísticas detalhadas sobre o processo de deduplicação de dados para um conjunto de armazenamentos de contêiner de diretório ou um conjunto de armazenamentos de contêiner em nuvem específico, conclua as etapas a seguir: 1. Na página Visão geral do Operations Center, passe o mouse sobre o ícone de configurações  e clique em **Construtor de comando**. 2. Obtenha um relatório estatístico emitindo o comando **GENERATE DEDUPSTATS**. Siga as instruções em GENERATE DEDUPSTATS (Gerar estatísticas de deduplicação de dados para um conjunto de armazenamentos de contêineres de diretório). 3. Visualize o relatório estatístico emitindo o comando **QUERY DEDUPSTATS**. Siga as instruções em QUERY DEDUPSTATS (Consultar estatísticas de deduplicação de dados).

Verifique se os arquivos de backup atuais para configuração do dispositivo e informações do histórico do volume foram salvos.	Acesse os locais de armazenamento para assegurar que os arquivos estejam disponíveis. O método preferencial é salvar os arquivos de backup em dois locais.
	
	Para localizar o histórico do volume e arquivos de configuração de dispositivo, conclua as etapas a seguir:
	1. Na página Visão geral do Operations Center, passe o mouse sobre o ícone de configurações  e clique em **Construtor de comando**.
	2. Para localizar o histórico do volume e arquivos de configuração de dispositivo, emita os seguintes comandos:
	`query option volhistory`
	`query option devconfig`
	3. Na saída, revise a coluna Configuração de opção para localizar os locais do arquivo.
	
	Se ocorrer um desastre, o arquivo do histórico de volume e o arquivo de configuração de dispositivo serão necessários para restaurar o banco de dados do servidor.	

Tabela 16. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas

Determine se há espaço suficiente disponível para o sistema de arquivos do diretório de instâncias.	Verifique se há pelo menos 20% de espaço livre disponível no sistema de arquivos de diretório de instâncias. Execute a ação apropriada para seu sistema operacional:
	• AIX Para visualizar o espaço disponível no sistema de arquivos, na linha de comandos do sistema operacional, emita o seguinte comando:
	`df -g instance_directory`
	em que *instance_directory* especifica o diretório de instâncias.
	• Linux Para visualizar o espaço disponível no sistema de arquivos, na linha de comandos do sistema operacional, emita o seguinte comando:
	`df -h instance_directory`
	em que *instance_directory* especifica o diretório de instâncias.
	• Windows No programa Windows Explorer, clique com o botão direito no sistema de arquivos e clique em **Propriedades**. Visualize as informações de capacidade.
	O local preferido do diretório de instâncias depende do sistema operacional em que o servidor está instalado:
	• AIX Linux `/home/tsminst1/tsminst1`
	• Windows `C:\tsminst1`
	Dica: Se você concluiu uma planilha de planejamento, o local do diretório de instâncias será registrado na planilha.	

Tabela 16. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Identifique a atividade do cliente inesperada.	Para monitorar a atividade de cliente para determinar se os volumes de dados excederam as quantidades esperadas, conclua as etapas a seguir: 1. Na página Visão geral do Operations Center, clique na área Clientes. 2. Para visualizar a atividade durante as duas últimas semanas, dê um clique duplo em qualquer cliente. 3. Para visualizar o número de bytes enviados ao cliente, clique na guia **Propriedades**. 4. Na área Última sessão, visualize a linha Enviados ao cliente.	Ao dar um clique duplo em um cliente na tabela Clientes, a área Atividade durante 2 semanas exibe a quantidade de dados que o cliente enviou ao servidor a cada dia. Revise periodicamente a tabela de resumo de atividade SQL que contém estatísticas sobre sessões do cliente. Para comparar a atividade atual com a atividade anterior, use uma instrução **SQL SELECT**. Se o nível de atividade for significativamente diferente da atividade anterior, isso poderá indicar um ataque de ransomware. Periodicamente, revise o log de atividades. Procure mensagens ANE que indiquem quantos arquivos foram submetidos a backup e inspecionados. Compare as taxas atuais de deduplicação de dados com as taxas anteriores. Se um número extraordinariamente alto de arquivos foi submetido a backup ou a taxa de deduplicação de dados cai inesperadamente para 0, isso pode indicar um ataque de ransomware.

Tabela 16. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Monitore o crescimento do conjunto de armazenamentos ao longo do tempo.	1. Na página Visão geral do Operations Center, clique na área Conjuntos. 2. Para visualizar a capacidade que foi usada durante as duas últimas semanas, selecione um conjunto e clique em **Detalhes**.	**Dicas:** • Para especificar o período que deve decorrer até que todas as extensões deduplicadas sejam removidas de um conjunto de armazenamentos de contêiner de diretório ou de um conjunto de armazenamentos de contêiner em nuvem após não serem mais referenciadas pelo inventário, conclua as seguintes etapas: 1. Na página **Conjuntos de armazenamentos** do Operations Center, selecione o conjunto de armazenamentos. 2. Clique em **Detalhes** > **Propriedades**. 3. Especifique a duração no campo `Período de atraso para reutilização do contêiner`. • Para determinar o desempenho da deduplicação de dados para conjuntos de armazenamentos de contêiner em diretório e de contêiner em nuvem, use o comando **`GENERATE DEDUPSTATS`**. • Para visualizar estatísticas de deduplicação de dados para um conjunto de armazenamentos, conclua as seguintes etapas: 1. Na página **Conjuntos de armazenamentos** do Operations Center, selecione o conjunto de armazenamentos. 2. Clique em **Detalhes** > **Propriedades**. Como alternativa, use o comando **`QUERY EXTENTUPDATES`** para exibir informações sobre atualizações em extensões de dados em conjuntos de armazenamentos de contêiner em diretório e de contêiner em nuvem. A saída de comando pode ajudá-lo a determinar quais extensões de dados não são mais referenciadas e quais são elegíveis para serem excluídas do sistema. Na saída, monitore o número de extensões de dados que podem ser excluídas do sistema. Essa métrica tem uma correlação direta com a quantidade de espaço livre que ficará disponível no conjunto de armazenamentos de contêiner. • Para exibir a quantidade de espaço físico que é ocupada por um espaço de arquivo após a remoção da economia da deduplicação de dados, use o comando **`select * from occupancy`**. A saída de comando inclui o valor LOGICAL_MB. LOGICAL_MB é a quantidade de espaço utilizado pelo espaço no arquivo.

Tabela 16. Tarefas de monitoramento periódicas (continuação)

Tarefa	Procedimentos básicos	Procedimentos avançados e resolução de problemas
Avalie a sincronização dos planejamentos de cliente. Certifique-se de que os horários de início e de encerramento de planejamentos de cliente atendam às suas necessidades de negócios.	Na página Visão geral do Operations Center, clique em **Clientes** > **Planejamentos**. Na tabela Planejamentos, a coluna Início exibe o horário de início configurado para a operação planejada. Para ver quando a operação mais recente foi iniciada, passe o mouse sobre o ícone de relógio.	**Dica:** É possível receber uma mensagem de aviso se uma operação do cliente for executada por mais tempo que o esperado. Execute as etapas a seguir: 1. Na página Visão geral do Operations Center, passe o mouse sobre **Clientes** e clique em **Planejamentos**. 2. Selecione um planejamento e clique em **Detalhes**. 3. Visualize os detalhes de um planejamento clicando na seta azul próxima à linha. 4. No campo **Alerta de tempo de execução**, especifique o horário em que uma mensagem de aviso será emitida se a operação planejada não for concluída. 5. Clique em **Salvar**.
Avalie a sincronização das tarefas de manutenção. Certifique-se de que os horários de início e de encerramento de tarefas de manutenção atendam às suas necessidades de negócios.	Na página Visão geral do Operations Center, clique em **Servidores** > **Manutenção**. Na tabela Manutenção, revise as informações na coluna Último tempo de execução. Para ver quando a última tarefa de manutenção foi iniciada, passe o mouse sobre o ícone de relógio.	**Dica:** Se uma tarefa de manutenção estiver sendo executada por muito tempo, altere o horário de início e o tempo de execução máximo. Execute as etapas a seguir: 1. Na página Visão geral do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Construtor de comando**. 2. Para alterar o horário de início ou o tempo de execução máximo para uma tarefa, emita o comando **UPDATE SCHEDULE**. Para obter instruções, consulte UPDATE SCHEDULE (Atualizar um planejamento do cliente).

Referências relacionadas:

- QUERY ACTLOG (Consultar o log de atividades)
- UPDATE STGPOOL (Atualizar um conjunto de armazenamentos)
- QUERY EXTENTUPDATES (Consultar extensões de dados atualizadas)

Capítulo 15. Verificando a conformidade da licença

Verifique se a solução do IBM Spectrum Protect está em conformidade com as disposições de seu contrato de licença. Ao verificar a conformidade regularmente, é possível controlar as tendências em crescimento de dados ou no uso da unidade de valor do processador (PVU). Use essas informações para planejar uma futura compra de licença.

Sobre Esta Tarefa

O método a ser usado para verificar se sua solução está em conformidade com os termos da licença varia de acordo com as disposições de seu contrato de licença do IBM Spectrum Protect.

Licenciamento de capacidade front-end
O modelo front-end determina os requisitos de licença com base na quantidade de dados primários que são relatados como sendo submetidos a backup por clientes. Os clientes incluem aplicativos, máquinas virtuais e sistemas.

Licenciamento de capacidade back-end
O modelo de backend determina os requisitos de licença com base nos terabytes de dados que são armazenados em conjuntos de armazenamentos primários e repositórios.

Dicas:

- Para assegurar a exatidão das estimativas de capacidade de front-end e backend, instale a versão mais recente do software cliente em cada nó cliente.
- As informações de capacidade de front-end e backend no Operations Center são para propósitos de planejamento e estimação.

Licenciamento de PVU
O modelo PVU é baseado no uso de PVUs por dispositivos do servidor.

Importante: Os cálculos de PVU que são fornecidos pelo IBM Spectrum Protect são considerados estimativas e não são ligados legalmente. As informações sobre licença de PVU que são relatadas pelo IBM Spectrum Protect não são consideradas um substituto aceitável para o IBM License Metric Tool. O IBM License Metric Tool foi desenvolvido para refletir o uso real. Por exemplo, após instalar o Cliente de backup-archive do IBM Spectrum Protect, a ferramenta conta o cliente somente após o primeiro uso.

Para obter as informações mais recentes sobre os modelos de licenciamento, consulte as informações sobre os detalhes e as licenças do produto no website da família de produtos do IBM Spectrum Protect. Se você tiver perguntas ou dúvidas sobre requisitos de licenciamento, entre em contato com o provedor de software do IBM Spectrum Protect.

Procedimento

Para monitorar a conformidade da licença, conclua as etapas que correspondem aos as disposições de seu contrato de licença.

Dica: O Operations Center fornece um relatório de e-mail que resume o uso de capacidade de front-end e backend. Os relatórios podem ser enviados automaticamente para um ou mais destinatários regularmente. Para configurar e gerenciar relatórios de e-mail, clique em **Relatórios** na barra de menus do Operations Center.

Opção	Descrição
Modelo front-end	1. Na barra de menus do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Licenciamento**. A estimativa de capacidade front-end é exibida na página Uso de front-end. 2. Se for exibido um valor na coluna Sem relatório, clique no número para identificar clientes que não relataram o uso de capacidade. 3. Para estimar a capacidade de clientes que não relataram o uso de capacidade, acesse o seguinte site de FTP, que fornece ferramentas e instruções de medição: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Para medir a capacidade de front-end por script, conclua as instruções no guia de licenciamento mais recente disponível. 4. Inclua a estimativa do Operations Center e todas as estimativas obtidas usando um script. 5. Verifique se a capacidade estimada está em conformidade com seu contrato de licença.
Modelo backend	**Restrição:** Se os servidores de replicação de origem e de destino não usarem as mesmas configurações de política, não será possível usar o Operations Center para monitorar o uso de capacidade de backend para clientes replicados. Para obter informações sobre como estimar o uso de capacidade para esses clientes, consulte a nota técnica 1656476. 1. Na barra de menus do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Licenciamento**. 2. Clique na guia **Back-end**. 3. Verifique se a quantidade estimada de dados está em conformidade com seu contrato de licença.
Modelo de PVU	Para obter informações sobre como avaliar a conformidade com os termos de licenciamento PVU, consulte Avaliando a conformidade com o modelo de licenciamento PVU.

Capítulo 16. Rastreando o status do sistema usando relatórios de e-mail

Configure o Operations Center para gerar relatórios de e-mail que resumem o status do sistema. É possível configurar uma conexão do servidor de e-mail, alterar configurações de relatório e, de modo opcional, criar relatórios customizados.

Antes de Iniciar

Antes de configurar relatórios de e-mail, certifique-se de que os requisitos a seguir sejam atendidos:

- Um servidor host do Protocolo Simples de Transporte de Correio (SMTP) está disponível para enviar e receber relatórios por email. O servidor SMTP deve ser configurado como uma retransmissão de e-mail aberta. Também é necessário assegurar que o servidor do IBM Spectrum Protect que envia emails tenha acesso ao servidor SMTP. Se o Operations Center for instalado em um computador separado, esse computador não precisará de acesso ao servidor SMTP.
- Para configurar relatórios de e-mail, deve-se ter privilégio no sistema para o servidor.
- Para especificar os destinatários, é possível inserir um ou mais endereços de email ou IDs de administrador. Se você deseja inserir um ID de administrador, o ID deve estar registrados no servidor do hub e deve ter um endereço de e-mail associado a ele. Para especificar um endereço de email para um administrador, use o parâmetro **EMAILADDRESS** do comando **UPDATE ADMIN**.

Sobre Esta Tarefa

É possível configurar o Operations Center para enviar um relatório de operações gerais, um relatório de conformidade da licença e um ou mais relatórios customizados. É possível criar relatórios customizados selecionando um modelo a partir de um conjunto de modelos de relatórios comumente usados ou inserindo instruções SQL SELECT para consultar servidores gerenciados.

Procedimento

Para configurar e gerenciar relatórios de e-mail, conclua as etapas a seguir:

1. Na barra de menus do Operations Center, clique em **Relatórios**.
2. Se uma conexão do servidor de e-mail ainda não estiver configurada, clique em**Configurar servidor de Correio** e complete os campos. Após você configurar o servidor de correio, o relatório de operações gerais e o relatório de conformidade da licença são ativados.
3. Para alterar configurações de relatório, selecione um relatório, clique em **Detalhes** e atualize o formulário.
4. Opcional: Para incluir um relatório customizado, clique em **+ Relatório**, e preencha os campos.

   Dica: Para executar e enviar um relatório imediatamente, selecione o relatório e clique em **Enviar**.

Resultados

Relatórios ativados são enviados de acordo com as configurações especificadas.

Referências relacionadas:

UPDATE ADMIN (Atualizar um Administrador)

Parte 4. Gerenciando operações para uma solução de disco multisite

Use estas informações para gerenciar operações para uma solução de disco multisite com o IBM Spectrum Protect que inclui um servidor e usa deduplicação de dados para vários locais.

Capítulo 17. Gerenciando o Operations Center

O Operations Center fornece acesso à web e por dispositivo móvel a informações de status sobre o ambiente do IBM Spectrum Protect. É possível usar o Operations Center para monitorar vários servidores e concluir algumas tarefas administrativas. O Operations Center também fornece acesso à web para a linha de comandos do IBM Spectrum Protect.

Incluindo e removendo servidores spoke

Em um ambiente de vários servidores, é possível conectar-se a outros servidores, denominados *servidores spoke*, para o servidor do hub.

Sobre Esta Tarefa

Os servidores spoke enviam alertas e informações de status para o servidor do hub. O Operations Center mostra uma visualização consolidada de alertas e informações de status para o servidor de hub e quaisquer servidores spoke.

Incluindo um Servidor spoke

Depois de configurar o servidor do hub para o Operations Center, é possível incluir um ou mais servidores spoke no servidor do hub.

Antes de Iniciar

A comunicação entre o servidor spoke e o servidor do hub deve ser assegurada usando o protocolo de Segurança da Camada de Transporte (TLS). Para uma comunicação segura, inclua o certificado do servior spoke no arquivo de armazenamento confiável do servidor do hub.

Procedimento

1. Na barra de menus Operations Center, clique em **Servidores**. A página Servidores se abre.

   Na tabela na página Servidores, um servidor pode ter um status de "Não monitorado". Este status significa que embora um administrador tenha definido esse servidor para o servidor de hub usando o comando **DEFINE SERVER**, o servidor ainda não está configurado como um servidor spoke.
2. Conclua uma das etapas a seguir:
   - Clique no servidor para destacá-lo e na barra de menus da tabela, clique em **Monitorar Spoke**.
   - Se o servidor que você deseja incluir não for mostrado na tabela e a comunicação segura do SSL/TLS não for necessária, clique em **+ Spoke** na barra de menus da tabela.
3. Forneça as informações necessárias e conclua as etapas no assistente de configuração do spoke.

   Dica: Se o período de retenção de registro de eventos do servidor for menor que 14 dias, o período será automaticamente reconfigurado para 14 dias se você configurar o servidor como um servidor spoke.

Removendo um servidor spoke

É possível remover um servidor spoke do Operations Center.

Sobre Esta Tarefa

Pode ser necessário remover um servidor spoke nas seguintes situações, por exemplo:

- Você deseja mover o servidor spoke de um servidor do hub para outro servidor do hub.
- Você deseja desatribuir o servidor spoke.

Procedimento

Para remover o servidor spoke do grupo de servidores que são gerenciados pelo servidor do hub, conclua as etapas a seguir:

1. Na linha de comandos do IBM Spectrum Protect, emita o comando a seguir no servidor do hub:

   ```
   QUERY MONITORSETTINGS
   ```

2. Na saída do comando, copie o nome que está no campo **Grupo monitorado**.
3. Emita o seguinte comando no servidor do hub, em que *group_name* representa o nome do grupo monitorado, e *member_name* representa o nome do servidor spoke:

   ```
   DELETE GRPMEMBER group_name member_name
   ```

4. Opcional: Se desejar mover o servidor spoke de um servidor do hub para outro servidor do hub, **não** conclua esta etapa. Caso contrário, você pode desativar o alerta e monitoramento no servidor spoke emitindo os seguintes comandos no servidor spoke:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Opcional: Se a definição do servidor spoke for usada para outros propósitos, como configuração corporativa, roteamento de comandos, armazenamento de volumes virtuais ou gerenciamento de bibliotecas, **não** conclua esta etapa. Caso contrário, será possível excluir a definição do servidor spoke no servidor do hub, emitindo o seguinte comando no servidor do hub:

   ```
   DELETE SERVER spoke_server_name
   ```

   Dica: Se uma definição do servidor for excluída imediatamente após o servidor ser removido do grupo monitorado, as informações de status para o servidor poderão permanecer no Operations Center indefinidamente.

   Para evitar esse problema, espere até o intervalo de coleta de status seja aprovado antes de excluir a definição do servidor. O intervalo de coleta de status é mostrado na página Configurações do Operations Center.

Iniciando e parando o servidor da web

O servidor da web do Operations Center é executado como um serviço e é iniciado automaticamente. Você pode precisar parar e iniciar o servidor da web, por exemplo, para fazer mudanças na configuração.

Procedimento

1. Para o servidor da Web.
   - AIX No diretório /*installation_dir*/ui/utils, em que *installation_dir* representa o diretório no qual o Operations Center está instalado, emita o comando a seguir:

     ```
     ./stopserver.sh
     ```
   - Linux Emita o seguinte comando:

     ```
     service opscenter.rc stop
     ```
   - Windows Na janela Serviços, pare o serviço **IBM Spectrum Protect Operations Center**.
2. Iniciar o servidor da Web.
   - AIX No diretório /*installation_dir*/ui/utils, em que *installation_dir* representa o diretório no qual o Operations Center está instalado, emita o comando a seguir:

     ```
     ./startserver.sh
     ```
   - Linux Emita os seguintes comandos:

     Inicie o servidor:

     ```
     service opscenter.rc start
     ```

     Reinicie o servidor:

     ```
     service opscenter.rc restart
     ```

     Determine se o servidor está em execução:

     ```
     service opscenter.rc status
     ```
   - Windows Na janela Serviços, inicie o serviço **IBM Spectrum Protect Operations Center**.

Reiniciando o assistente de configuração inicial

Pode ser necessário reiniciar o assistente inicial do Operations Center, por exemplo, para fazer mudanças na configuração.

Antes de Iniciar

Para alterar as seguintes configurações, use a página Configurações no Operations Center em vez de reiniciar o assistente de configuração inicial:

- A frequência com que os dados de status são atualizados
- A duração em que os alertas permanecem ativos, inativos ou fechados
- As condições que indicam que os clientes estão em risco

A ajuda do Operations Center inclui informações adicionais sobre como alterar essas configurações.

Sobre Esta Tarefa

Para reiniciar o assistente de configuração inicial, deve-se excluir um arquivo de propriedades que inclui informações sobre a conexão do servidor do hub. No entanto, as configurações de alerta, monitoramento, em risco ou multisservidor que foram definidas para o servidor do hub não são excluídas. Estas configurações são usadas como as configurações padrão no assistente de configuração quando o assistente é reiniciado.

Procedimento

1. Pare o servidor da web Operations Center.
2. No computador em que o Operations Center está instalado, acesse o seguinte diretório, em que *installation_dir* representa o diretório no qual o Operations Center está instalado:
   - AIX Linux *installation_dir*/ui/Liberty/usr/servers/guiServer
   - Windows *installation_dir*\ui\Liberty\usr\servers\guiServer

   Por exemplo:
   - AIX Linux /opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Windows c:\Program Files\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. No diretório guiServer, exclua o arquivo serverConnection.properties.
4. Inicie o servidor da web Operations Center.
5. Abra o Operations Center.
6. Use o assistente de configuração para reconfigurar o Operations Center. Especifique uma nova senha para o ID de administrador de monitoramento.
7. Em quaisquer servidores spoke que foram anteriormente conectados ao servidor do hub, atualize a senha para o ID de administrador de monitoramento emitindo o seguinte comando a partir da interface da linha de comandos do IBM Spectrum Protect:

   ```
   UPDATE ADMIN IBM-OC-hub_server_name new_password
   ```

   Restrição: Não altere nenhuma outra configuração para esse ID de administrador. Após especificar a senha inicial, essa senha é gerenciada automaticamente pelo Operations Center.

Alterando o servidor do hub

É possível usar o Operations Center para remover o servidor do hub do IBM Spectrum Protect e configurar outro servidor do hub.

Procedimento

1. Reinicie o assistente de configuração inicial do Operations Center. Como parte desse procedimento, você exclui a conexão do servidor do hub existente.
2. Use o assistente para configurar o Operations Center para conectar-se ao novo servidor do hub.

Tarefas relacionadas:

"Reiniciando o assistente de configuração inicial" na página 109

Restaurando a configuração para o estado de pré-configuração

Se ocorrerem alguns problemas, talvez você queira restaurar a configuração do Operations Center para o estado pré-configurado em que os servidores do IBM Spectrum Protect não estão definidos como servidores do hub ou spoke.

Procedimento

Para restaurar a configuração, conclua as etapas a seguir:

1. Pare o servidor da web Operations Center.
2. Desconfigure o servidor do hub concluindo as etapas a seguir:
   a. No servidor do hub, emita os seguintes comandos:

      ```
      SET MONITORINGADMIN ""
      SET MONITOREDSERVERGROUP ""
      SET STATUSMONITOR OFF
      SET ALERTMONITOR OFF
      REMOVE ADMIN IBM-OC-hub_server_name
      ```

      Dica: IBM-OC-*hub_server_name* representa o ID de administrador de monitoramento que foi criado automaticamente quando o servidor do hub foi configurado inicialmente.
   b. Reconfigure a senha para o servidor do hub emitindo o seguinte comando no servidor do hub:

      ```
      SET SERVERPASSWORD ""
      ```

      Atenção: Não conclua essa etapa se o servidor do hub estiver configurado com outros servidores para outros propósitos, como compartilhamento de biblioteca, exportação e importação de dados ou replicação de nó.
3. Desconfigure os servidores spoke concluindo as etapas a seguir:
   a. No servidor do hub, para determinar se alguns dos servidores spoke permanecem como membros do grupo de servidores, emita o seguinte comando:

      ```
      QUERY SERVERGROUP IBM-OC-hub_server_name
      ```

      Dica: IBM-OC-*hub_server_name* representa o nome do grupo de servidores monitorados que foi criado automaticamente durante a configuração do primeiro servidor spoke. Este nome do grupo de servidores também é igual ao ID de administrador de monitoramento que foi criado automaticamente quando o servidor do hub foi configurado inicialmente.
   b. No servidor do hub, para excluir servidores spoke do grupo de servidores, emita o seguinte comando para cada servidor spoke:

      ```
      DELETE GRPMEMBER IBM-OC-hub_server_name spoke_server_name
      ```
   c. Após a exclusão de todos os servidores spoke do grupo de servidores, emita os seguintes comandos no servidor do hub:

      ```
      DELETE SERVERGROUP IBM-OC-hub_server_name
      SET MONITOREDSERVERGROUP ""
      ```
   d. Em cada servidor spoke, emita os seguintes comandos:

      ```
      REMOVE ADMIN IBM-OC-hub_server_name
      SETOPT PUSHSTATUS NO
      SET ALERTMONITOR OFF
      SET STATUSMONITOR OFF
      ```
   e. Em cada servidor spoke, exclua a definição do servidor do hub emitindo o seguinte comando:

      ```
      DELETE SERVER hub_server_name
      ```

Atenção: Não conclua essa etapa se a definição for usada para outros propósitos, como compartilhamento de biblioteca, exportação e importação de dados ou replicação de nó.

f. No servidor do hub, exclua a definição de cada servidor spoke emitindo o seguinte comando:

```
DELETE SERVER spoke_server_name
```

Atenção: Não conclua essa etapa se a definição do servidor for usada para outros propósitos, como compartilhamento de biblioteca, exportação e importação de dados ou replicação de nó.

4. Restaure as configurações padrão em cada servidor emitindo os seguintes comandos:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Reinicie o assistente de configuração inicial do Operations Center.

Tarefas relacionadas:

"Reiniciando o assistente de configuração inicial" na página 109

"Iniciando e parando o servidor da web" na página 109

Capítulo 18. Protegendo aplicativos, máquinas virtuais e sistemas

O servidor protege dados para clientes, que podem incluir aplicativos, máquinas virtuais e sistemas. Para começar a proteger dados de cliente, registre o nó cliente no servidor e selecione um planejamento de backup para proteger os dados de cliente.

Incluindo clientes

Após implementar uma solução de proteção de dados com o IBM Spectrum Protect, é possível expandir a solução incluindo clientes.

Sobre Esta Tarefa

O procedimento descreve as etapas básicas para a inclusão de um cliente. Para obter instruções mais específicas sobre como configurar clientes, consulte a documentação para o produto instalado no nó cliente. É possível ter os seguintes tipos de nós clientes:

Nós clientes do aplicativo
Os nós clientes do aplicativo incluem servidores de email, bancos de dados e outros aplicativos. Por exemplo, qualquer um dos seguintes aplicativos pode ser um nó cliente do aplicativo:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nós clientes do sistema
Os nós clientes do sistema incluem estações de trabalho, servidores de arquivos de armazenamento conectado à rede (NAS) e clientes da API.

Nós clientes de máquina virtual
Os nós clientes de máquina virtual consistem em um host convidado individual em um hypervisor. Cada máquina virtual é representada como um espaço no arquivo.

Procedimento

Para incluir um cliente, conclua as etapas a seguir:

1. Selecione o software a ser instalado no nó cliente e planeje a instalação. Siga as instruções em “Selecionando o software cliente e planejando a instalação” na página 114.
2. Especifique como fazer backup e arquivar dados de cliente. Siga as instruções em “Especificando regras para backup e arquivamento de dados de cliente” na página 115.
3. Especifique quando fazer backup e arquivar dados de cliente. Siga as instruções em “Planejando operações de backup e archive” na página 119.
4. Para permitir que o cliente se conecte ao servidor, registre o cliente. Siga as instruções em “Registrando clientes” na página 120.

5. Para começar a proteger um nó cliente, instale e configure o software selecionado no nó cliente. Siga as instruções em “Instalando e configurando clientes” na página 121.

Selecionando o software cliente e planejando a instalação

Diferentes tipos de dados requerem diferentes tipos de proteção. Identifique o tipo de dados que devem ser protegidos e selecione o software apropriado.

Sobre Esta Tarefa

A prática preferencial é instalar o cliente de backup-archive em todos os nós clientes para que seja possível configurar e iniciar o client acceptor no nó cliente. O client acceptor é projetado para executar operações planejadas de forma eficiente.

O client acceptor executa planejamentos para os produtos a seguir: o cliente de backup-archive, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail e IBM Spectrum Protect for Virtual Environments. Se você instalar um produto para o qual o client acceptor não executa planejamentos, deverá seguir as instruções de configuração na documentação do produto para assegurar que as operações planejadas possam ocorrer.

Procedimento

Com base em seu objetivo, selecione o produto a ser instalado e revise as instruções de instalação.

Dica: Se você instalar o software cliente agora, também deverá concluir as tarefas de configuração do cliente que estão descritas em “Instalando e configurando clientes” na página 121 antes de poder usar o cliente.

Objetivo	Produto e descrição	Instruções de instalação
Proteger um servidor de arquivos ou estação de trabalho	O cliente de backup-archive faz backup e arquiva os arquivos e diretórios de servidores de arquivos e estações de trabalho para armazenamento. Também é possível restaurar e recuperar versões de backup e cópias de arquivos arquivadas.	• Requisitos do cliente de backup-archive • Instale deus clientes de archive de backup do UNIX e do Linux • Instalando o cliente Windows pela primeira vez
Proteger aplicativos com recursos de backup e restauração de captura instantânea	O IBM Spectrum Protect Snapshot protege dados com recursos integrados de backup e restauração de captura instantânea direcionados ao aplicativo. É possível proteger dados que são armazenados pelo IBM Db2 software de banco de dados e aplicativos SAP, Oracle, Microsoft Exchange e Microsoft SQL Server.	• Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para UNIX e Linux • Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para VMware • Instalando e Atualizando o IBM Spectrum Protect Snapshot para Windows
Proteja um aplicativo de e-mail em um servidor IBM Domino	O IBM Spectrum Protect for Mail: Data Protection for IBM Domino automatiza a proteção de dados para que os backups sejam concluídos sem encerrar servidores IBM Domino.	• Instalação do Data Protection for IBM Domino em um sistema UNIX, AIX ou Linux (V7.1.0) • Instalação do Data Protection for IBM Domino em um sistema Windows (V7.1.0)
Proteja um aplicativo de e-mail em um servidor Microsoft Exchange	O IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatiza a proteção de dados para que os backups sejam concluídos sem encerrar servidores Microsoft Exchange.	Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

Objetivo	Produto e descrição	Instruções de instalação
Proteja um banco de dados do Db2	A interface de programação de aplicativos (API) do cliente de backup e archive pode ser usada para fazer backup de dados do Db2 para o servidor IBM Spectrum Protect.	Instalando clientes de archive de backup do IBM Spectrum Protect (UNIX, Linux e Windows)
Proteja um banco de dados IBM Informix	A API do cliente de backup-archive pode ser usada para fazer backup de dados do Informix no servidor IBM Spectrum Protect.	Instalando clientes de archive de backup do IBM Spectrum Protect (UNIX, Linux e Windows)
Proteja um banco de dados Microsoft SQL	O IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protege dados do Microsoft SQL.	Instalando o Data Protection for SQL Server no Núcleo do Sistema Windows
Proteger um banco de dados Oracle	O IBM Spectrum Protect for Databases: Data Protection for Oracle protege dados do Oracle.	Instalação do Data Protection for Oracle
Proteger um ambiente SAP	O IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP fornece proteção customizada para ambientes SAP. O produto foi projetado para melhorar a disponibilidade de servidores de banco de dados SAP e reduzir a carga de trabalho de administração.	• Instalando a proteção de dados para o SAP para Db2 • Instalando o Data Protection for SAP for Oracle
Proteger uma máquina virtual	O IBM Spectrum Protect for Virtual Environments fornece proteção que é customizada para ambientes virtuais Microsoft Hyper-V e VMware. É possível usar o IBM Spectrum Protect for Virtual Environments para criar backups incrementais contínuos que estão armazenados e um servidor centralizado, criar políticas de backup e restaurar máquinas virtuais ou arquivos individuais. Como alternativa, use o cliente de backup-archive para fazer backup e restaurar uma máquina virtual integral do VMware ou Microsoft Hyper-V. Também é possível fazer backup e restaurar arquivos ou diretórios a partir de uma máquina virtual VMware.	• Instalando o Data Protection for Microsoft Hyper-V • Instalando e Atualizando o Proteção de Dados para VMware • Instalando clientes de archive de backup do IBM Spectrum Protect (UNIX, Linux e Windows)

Dica: Para usar o cliente para gerenciamento de espaço, é possível instalar o IBM Spectrum Protect for Space Management ou o IBM Spectrum Protect HSM for Windows.

Especificando regras para backup e arquivamento de dados de cliente

Antes de incluir um cliente, assegure-se de que as regras sejam especificadas para operações de backup e archive para os dados de cliente. Durante o processo de registro do cliente, você atribua o nó cliente a um domínio de política, que tem as regras que controlam como e quando os dados de cliente são armazenados.

Antes de Iniciar

Determine como continuar:

- Se estiver familiarizado com as políticas que estão configuradas para sua solução e souber que elas não requerem mudanças, continue com "Planejando operações de backup e archive" na página 119.
- Se não estiver familiarizado com as políticas, siga as etapas nesse procedimento.

Sobre Esta Tarefa

As políticas afetam a quantidade de dados que são armazenados ao longo do tempo e por quanto tempo os dados ficam retidos e disponíveis para restauração. Para atender aos objetivos de proteção de dados, é possível atualizar a política padrão e criar suas próprias políticas. Uma política inclui as seguintes regras:

- Como e quando os arquivos são submetidos a backup e arquivados no armazenamento do servidor.
- O número de cópias de um arquivo e o período pelo qual as cópias são mantidas no armazenamento do servidor.

Durante o processo de registro do cliente, você designa um cliente a um *domínio de política*. A política para um cliente específico é determinada pelas regras no domínio de política ao qual o cliente está designado. No domínio de política, as regras que estão em vigor estão no *conjunto de políticas* ativas.

Quando um cliente faz backup ou arquiva um arquivo, o arquivo é ligado a uma classe de gerenciamento no conjunto de políticas ativas do domínio de política. Uma *classe de gerenciamento* é o conjunto de chaves de regras para gerenciar dados de cliente. As operações de backup e archive no cliente usam as configurações na classe de gerenciamento padrão do domínio de política, a menos que você customize ainda mais a política. Uma política pode ser customizada definindo mais classes de gerenciamento e designando seu uso por meio de opções do cliente.

As opções do cliente podem ser especificadas em um arquivo local, editável no sistema do cliente e em um conjunto de opções do cliente no servidor. As opções no conjunto de opções do cliente no servidor podem substituir ou incluir nas opções no arquivo de opções do cliente local.

Procedimento

1. Revise as políticas que estão configuradas para sua solução seguindo as instruções em "Visualizando políticas" na página 117.
2. Se precisar fazer pequenas mudanças para atender aos requisitos de retenção de dados, siga as instruções em "Editando políticas" na página 117.
3. Opcional: Se precisar criar domínios de política ou fazer mudanças extensivas nas políticas para atender aos requisitos de retenção de dados, consulte Customizando políticas.

Visualizando políticas

Visualize políticas para determinar se elas devem ser editadas para atender às suas necessidades.

Procedimento

1. Para visualizar o conjunto de políticas ativas para um domínio de política, conclua as etapas a seguir:
   a. Na página Serviços do Operations Center, selecione um domínio de política e clique em **Detalhes**.
   b. Na página Resumo do domínio de política, clique na guia **Conjuntos de políticas**.

      Dica: Para ajudar a assegurar que seja possível recuperar dados após um ataque de ransomware, aplique as seguintes diretrizes:

      - Assegure-se de que o valor na coluna Backups seja no mínimo de 2. O valor preferencial é 3, 4 ou mais.
      - Assegure-se de que o valor na coluna Manter backups extras seja no mínimo de 14 dias. O valor preferencial é 30 ou mais dias.
      - Assegure-se de que o valor na coluna Manter archives seja no mínimo de 30 dias.

      Se o software IBM Spectrum Protect for Space Management está instalado no cliente, assegure-se de que os dados sejam submetidos a backup antes de migrá-lo. No comando **DEFINE MGMTCLASS** ou **UPDATE MGMTCLASS**, especifique **MIGREQUIRESBKUP=YES**. Em seguida, siga as diretrizes na dica.
2. Para visualizar conjuntos de políticas inativas para um domínio de política, conclua as seguintes etapas:
   a. Na página Conjuntos de políticas, clique na alternância **Configurar**. Agora é possível visualizar e editar os conjuntos de políticas que estão inativas.
   b. Role pelos conjuntos de políticas inativas usando as setas para avançar e voltar. Ao visualizar um conjunto de políticas inativas, as configurações que diferenciam o conjunto de políticas inativas do conjunto de políticas ativas são destacadas.
   c. Clique na alternância **Configurar**. Os conjuntos de políticas não são mais editáveis.

Editando políticas

Para alterar as regras que se aplicam a um domínio de política, edite o conjunto de políticas ativas para o domínio de política. Também é possível ativar um conjunto de políticas diferente para um domínio.

Antes de Iniciar

As mudanças na política podem afetar a retenção de dados. Certifique-se de continuar fazendo backup de dados que são essenciais para sua organização para que seja possível restaurar esses dados se ocorrer um desastre. Além disso, certifique-se de que seu sistema tenha espaço de armazenamento suficiente para operações de backup planejadas.

Sobre Esta Tarefa

Edite um conjunto de políticas alterando uma ou mais classes de gerenciamento no conjunto de políticas. Se editar o conjunto de políticas ativas, as mudanças não

estarão disponíveis para os clientes, a menos que você reative o conjunto de políticas. Para disponibilizar o conjunto de políticas editadas para os clientes, ative o conjunto de políticas.

Embora seja possível definir vários conjuntos de políticas para um domínio de política, apenas um conjunto de políticas pode estar ativo. Ao ativar um conjunto de políticas diferente, ele substitui o conjunto de políticas ativas atualmente.

Para saber sobre práticas preferenciais para definir políticas, consulte Customizando políticas.

Procedimento

1. Na página Serviços do Operations Center, selecione um domínio de política e clique em **Detalhes**.
2. Na página Resumo do domínio de política, clique na guia **Conjuntos de políticas**.

   A página Conjuntos de políticas indica o nome do conjunto de políticas ativas e lista todas as classes de gerenciamento para esse conjunto de políticas.
3. Clique na alternância **Configurar**. O conjunto de políticas é editável.
4. Opcional: Para editar um conjunto de políticas que não está ativo, clique nas setas avançar e voltar para localizar o conjunto de políticas.
5. Edite o conjunto de políticas concluindo qualquer uma das seguintes ações:

Opção	Descrição
Incluir uma classe de gerenciamento	1. Na tabela Conjuntos de políticas, clique em **+Classe de gerenciamento**. 2. Para especificar as regras para fazer backup e arquivar dados, preencha os campos na janela Incluir classe de gerenciamento. 3. Para tornar a classe de gerenciamento a classe de gerenciamento padrão, selecione a caixa de seleção **Tornar padrão**. 4. Clique em **Incluir**.
Excluir uma classe de gerenciamento	Na coluna Classe de gerenciamento, clique em **-**. **Dica:** Para excluir a classe de gerenciamento padrão, primeiro você deve designar uma classe de gerenciamento diferente como o padrão.
Tornar uma classe de gerenciamento a classe de gerenciamento padrão	Na coluna Padrão para a classe de gerenciamento, clique no botão de opções. **Dica:** A classe de gerenciamento padrão gerencia arquivos do cliente quando outra classe de gerenciamento não está designada ou não é apropriada para gerenciar um arquivo. Para assegurar que os clientes sempre possam fazer backup e arquivar arquivos, escolha uma classe de gerenciamento padrão que contenha regras para fazer backup e arquivar arquivos.
Modificar uma classe de gerenciamento	Para alterar as propriedades de uma classe de gerenciamento, atualize os campos na tabela.

6. Clique em **Salvar**.

   Atenção: Ao ativar um novo conjunto de políticas, os dados podem ser perdidos. Os dados que estão protegidos em um conjunto de políticas podem não ser protegidos em outro conjunto de políticas. Portanto, antes de ativar um conjunto de políticas, certifique-se de que as diferenças entre o conjunto de políticas anterior e o novo conjunto de políticas não causem perda de dados.

7. Clique em **Ativar**. É exibido um resumo das diferenças entre o conjunto de políticas ativas e o novo conjunto de políticas. Certifique-se de que as mudanças no novo conjunto de políticas sejam consistentes com seus requisitos de retenção de dados, concluindo as etapas a seguir:
   a. Revise as diferenças entre as classes de gerenciamento correspondentes nos dois conjuntos de políticas e considere as consequências para arquivos do cliente. Os arquivos do cliente que estão ligados às classes de gerenciamento no conjunto de políticas ativas serão ligados às classes de gerenciamento com os mesmos nomes no novo conjunto de políticas.
   b. Identifique classes de gerenciamento no conjunto de políticas ativas que não possuem contrapartes no novo conjunto de políticas e considere as consequências para arquivos do cliente. Os arquivos do cliente que estão ligados a essas classes de gerenciamento serão gerenciados pela classe de gerenciamento padrão no novo conjunto de políticas.
   c. Se as mudanças a serem implementadas pelo conjunto de políticas forem aceitáveis, selecione a caixa de seleção **Entendo que essas atualizações podem causar perda de dados** e clique em **Ativar**.

Planejando operações de backup e archive

Antes de registrar um novo cliente no servidor, certifique-se de que um planejamento esteja disponível para especificar quando ocorrerão as operações de backup e archive. Durante o processo de registro, você designa um planejamento ao cliente.

Antes de Iniciar

Determine como continuar:

- Se estiver familiarizado com os planejamentos que estão configurados para a solução e souber que eles não requerem modificação, continue com "Registrando clientes" na página 120.
- Se não estiver familiarizado com os planejamentos ou os planejamentos precisarem de modificação, siga as etapas nesse procedimento.

Sobre Esta Tarefa

Geralmente as operações de backup para todos os clientes devem ser concluídas diariamente. Planeje as cargas de trabalho do cliente e do servidor para atingir o melhor desempenho para o seu ambiente de armazenamento. Para evitar a sobreposição de operações do cliente e do servidor, considere planejar operações de backup e archive do cliente para execução durante a noite. Se as operações do cliente e do servidor se sobrepuserem ou não tiverem tempo e recursos suficientes para serem processadas, pode ocorrer diminuição do desempenho do sistema, operações com falha e outros problemas.

Procedimento

1. Revise os planejamentos disponíveis passando o mouse sobre **Clientes** na barra de menus do Operations Center. Clique em **Planejamentos**.
2. Opcional: Modifique ou crie um planejamento concluindo as etapas a seguir:

Opção	Descrição
Modificar um planejamento	1. Na visualização Planejamentos, selecione o planejamento e clique em **Detalhes**. 2. Na página Detalhes do planejamento, visualize detalhes clicando nas setas azuis no início das linhas. 3. Modifique as configurações no planejamento e clique em **Salvar**.
Criar um planejamento	Na visualização Planejamentos, clique em **+Planejamento** e conclua as etapas para criar um planejamento.

3. Opcional: Para definir as configurações de planejamento que não estão visíveis no Operations Center, use um comando do servidor. Por exemplo, talvez você queira planejar uma operação do cliente que faça backup de um diretório específico e designe-o a uma classe de gerenciamento diferente do padrão.
   a. Na página Visão geral do Operations Center, passe o mouse sobre o ícone de configurações e clique em **Construtor de comando**.
   b. Emita o comando **DEFINE SCHEDULE** para criar um planejamento ou o comando **UPDATE SCHEDULE** para modificar um planejamento. Para obter mais informações sobre os comandos, veja DEFINE SCHEDULE (Definir um Planejamento de Cliente) ou UPDATE SCHEDULE (Atualizar um planejamento do cliente).

Tarefas relacionadas:

Ajustando o Planejamento para Operações Diárias

Registrando clientes

Registre um cliente para assegurar que ele possa se conectar ao servidor e o servidor possa proteger os dados de cliente.

Antes de Iniciar

Determine se o cliente requer um ID do usuário administrativo com autoridade do proprietário cliente no nó cliente. Para determinar quais clientes requerem um ID do usuário administrativo, consulte a nota técnica 7048963.

Restrição: Para alguns tipos de clientes, o nome do nó cliente e o ID do usuário administrativo devem corresponder. Não é possível autenticar esses clientes usando o método de autenticação Lightweight Directory Access Protocol que foi introduzido na V7.1.7. Para obter detalhes sobre esse método de autenticação, às vezes referido como modo integrado, consulte Autenticando usuários usando um banco de dados do Active Directory.

Procedimento

Para registrar um cliente, conclua uma das seguintes ações.

- Se o cliente requerer um ID do usuário administrativo, registre o cliente usando o comando **REGISTER NODE** e especifique o parâmetro **USERID**:

  ```
  register node node_name password userid=node_name
  ```

  em que *node_name* especifica o nome do nó e *password* especifica a senha do nó. Para obter detalhes, consulte a seção Registrar um Nó.

- Se o cliente não requerer um ID de usuário administrativo, registre o cliente usando o assistente Incluir Cliente do Operations Center. Execute as etapas a seguir:
  1. Na barra de menus do Operations Center, clique em **Clientes**.
  2. Na tabela Clientes, clique em **+ Cliente**.
  3. Conclua as etapas no assistente Incluir cliente:
     a. Especifique se os dados redundantes podem ser eliminados no cliente e no servidor. Na área de deduplicação de dados do lado do cliente, selecione a caixa de seleção **Ativar**.
     b. Na janela Configuração, copie os valores das opções **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** e **DEDUPLICATION**.

        Dica: Registre os valores da opção e mantenha-os em um local seguro. Após concluir o registro do cliente e instalar o software no nó cliente, use os valores para configurar o cliente.
     c. Siga as instruções no assistente para especificar o domínio de política, planejamento e conjunto de opções.
     d. Configure como os riscos são exibidos para o cliente, especificando a configuração em risco.
     e. Clique em **Incluir cliente**.

Referências relacionadas:

- Opção Tcpserveraddress
- Opção de tcpport
- Opção de nome do nó
- Opção deduplication

Instalando e configurando clientes

Para começar a proteger um nó cliente, deve-se instalar e configurar o software selecionado.

Procedimento

Se você já tiver instalado o software, inicie na etapa 2 na página 122.

1. Execute uma das seguintes ações:
   - Para instalar o software em um aplicativo ou nó cliente, siga as instruções.

Software	Link para instruções
Cliente de backup-archive do IBM Spectrum Protect	• Instale deus clientes de archive de backup do UNIX e do Linux • Instalando o cliente Windows pela primeira vez **Dica:** Também é possível atualizar clientes existentes usando o Operations Center. Para obter instruções, consulte Planejando atualizações do cliente.
IBM Spectrum Protect for Databases	• Instalação do Data Protection for Oracle • Instalando o Data Protection for SQL Server no Núcleo do Sistema Windows

Software	Link para instruções
IBM Spectrum Protect for Mail	• Instalação do Data Protection for IBM Domino em um sistema UNIX, AIX ou Linux (V7.1.0) • Instalação do Data Protection for IBM Domino em um sistema Windows (V7.1.0) • Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	• Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para UNIX e Linux • Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para VMware • Instalando e Atualizando o IBM Spectrum Protect Snapshot para Windows
IBM Spectrum Protect for Enterprise Resource Planning	• Instalando a proteção de dados para o SAP para Db2 • Instalando o Data Protection for SAP for Oracle

- Para instalar o software em um nó cliente de máquina virtual, siga as instruções para o tipo de backup selecionado.

Tipo de backup	Link para instruções
Se você planeja criar backups completos do VMware de máquinas virtuais, instale e configure o cliente de backup-archive do IBM Spectrum Protect.	• Instale deus clientes de archive de backup do UNIX e do Linux • Instalando o cliente Windows pela primeira vez
Se você planeja criar backups completos incrementais contínuos de máquinas virtuais, instale e configure o IBM Spectrum Protect for Virtual Environments e o cliente de backup-archive no mesmo nó cliente ou em nós clientes diferentes.	• Documentação on-line do produto IBM Spectrum Protect for Virtual Environments **Dica:** É possível obter o software para o IBM Spectrum Protect for Virtual Environments e o cliente de backup-archive no pacote de instalação do IBM Spectrum Protect for Virtual Environments.

2. Para permitir que o cliente se conecte ao servidor, inclua ou atualize os valores para as opções **TCPSERVERADDRESS**, **TCPPORT** e **NODENAME** no arquivo de opções do cliente. Use os valores registrados durante o registro do cliente (“Registrando clientes” na página 120).
   - Para clientes instalados em um sistema operacional AIX, Linux ou Mac OS X, inclua os valores no arquivo de opções do sistema do cliente, `dsm.sys`.
   - Para clientes que estão instalados em um sistema operacional Windows, inclua os valores no arquivo `dsm.opt`.

   Por padrão, os arquivos de opções estão no diretório de instalação.
3. Se você instalou um cliente de backup-archive em um sistema operacional Linux ou Windows, instale o client management service no cliente. Siga as instruções em “Instalando o serviço de gerenciamento de clientes” na página 70.
4. Configure o cliente para executar operações planejadas. Siga as instruções em “Configurando o cliente para executar operações planejadas” na página 123.

5. Opcional: Configure comunicações através de um firewall. Siga as instruções em “Configurando as comunicações entre o servidor e o cliente por meio de um firewall” na página 125.
6. Execute um backup de teste para verificar se os dados estão protegidos conforme planejado. Por exemplo, para um cliente de backup-archive, conclua as etapas a seguir:
   a. Na página Clientes do Operations Center, selecione o cliente do qual você deseja fazer backup e clique em **Fazer backup**.
   b. Verifique se o backup foi concluído com sucesso e se não há mensagens de aviso ou de erro.
7. Monitore os resultados das operações planejadas para o cliente no Operations Center.

O que Fazer Depois

Para mudar do que está sendo feito backup no cliente, siga as instruções em “Modificando o escopo de um backup de cliente” na página 130.

Configurando o cliente para executar operações planejadas

Deve-se configurar e iniciar um planejador de cliente no nó cliente. O planejador de cliente permite a comunicação entre o cliente e servidor para que operações planejadas possam ocorrer. Por exemplo, as operações planejadas geralmente incluem fazer backup de arquivos a partir de um cliente.

Sobre Esta Tarefa

O método preferencial é instalar o cliente de backup-archive em todos os nós clientes para que seja possível configurar e iniciar o client acceptor no nó cliente. O client acceptor é projetado para executar operações planejadas de forma eficiente. O client acceptor gerencia o planejador de cliente para que o planejador seja executado apenas quando necessário:

- Quando for tempo de consultar o servidor sobre a próxima operação planejada
- Quando for tempo de iniciar a próxima operação planejada

Ao usar o client acceptor, é possível reduzir o número de processos de segundo plano no cliente e ajudar a evitar problemas de retenção de memória.

O client acceptor executa planejamentos para os produtos a seguir: o cliente de backup-archive, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail e IBM Spectrum Protect for Virtual Environments. Se você instalou um produto para o qual o client acceptor não executa planejamentos, siga as instruções de configuração na documentação do produto para assegurar que as operações planejadas possam ocorrer.

Se seu negócio usar uma ferramenta de planejamento de terceiros como prática padrão, será possível usar essa ferramenta de planejamento como uma alternativa para o client acceptor. Geralmente, as ferramentas de planejamento de terceiros iniciam programas clientes diretamente usando comandos do sistema operacional. Para configurar uma ferramenta de planejamento de terceiros, consulte a documentação do produto.

Procedimento

Para configurar e iniciar o planejador de cliente usando o client acceptor, siga as instruções para o sistema operacional instalado no nó cliente:

AIX e Oracle Solaris

1. Na GUI do cliente de backup-archive, clique em **Editar** > **Preferências do cliente**.
2. Clique na guia **Web client**.
3. No campo **Opções de serviços gerenciados**, clique em **Planejar**. Se você também quiser que o client acceptor gerencie o Web client, clique na opção **Ambos**.
4. Para assegurar que o planejador possa iniciar de forma não assistida, no arquivo `dsm.sys`, configure a opção **`passwordaccess`** como `generate`.
5. Para armazenar a senha de nó do cliente, emita o seguinte comando e insira a senha de nó do cliente quando solicitada:

   ```
   dsmc query sess
   ```

6. Inicie o client acceptor emitindo o comando a seguir na linha de comandos:

   ```
   /usr/bin/dsmcad
   ```

7. Para permitir que o client acceptor seja iniciado automaticamente após uma reinicialização do sistema, inclua a entrada a seguir no arquivo de inicialização do sistema (geralmente, `/etc/inittab`):

   ```
   tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Client Acceptor Daemon
   ```

Linux

1. Na GUI do cliente de backup-archive, clique em **Editar** > **Preferências do cliente**.
2. Clique na guia **Web client**.
3. No campo **Opções de serviços gerenciados**, clique em **Planejar**. Se você também quiser que o client acceptor gerencie o Web client, clique na opção **Ambos**.
4. Para assegurar que o planejador possa iniciar de forma não assistida, no arquivo `dsm.sys`, configure a opção **`passwordaccess`** como `generate`.
5. Para armazenar a senha de nó do cliente, emita o seguinte comando e insira a senha de nó do cliente quando solicitada:

   ```
   dsmc query sess
   ```

6. Inicie o client acceptor efetuando login com o ID do usuário raiz e emitindo o comando a seguir:

   ```
   service dsmcad start
   ```

7. Para permitir que o client acceptor seja iniciado automaticamente após uma reinicialização do sistema, inclua o serviço emitindo o comando a seguir em um prompt de shell:

   ```
   # chkconfig --add dsmcad
   ```

MAC OS X

1. Na GUI do cliente de backup-archive, clique em **Editar** > **Preferências do cliente**.
2. Para assegurar que o planejador possa iniciar de forma não assistida, clique em **Autorização**, selecione **Geração de Senha** e clique em **Aplicar**.

3. Para especificar como os serviços são gerenciados, clique em **Web Client**, selecione **Planejar**, clique em **Aplicar** e clique em **OK**.
4. Para assegurar que a senha gerada seja salva, reinicie o cliente de backup-archive.
5. Use o aplicativo IBM Spectrum Protect Tools for Administrators para iniciar o client acceptor.

Windows

1. Na GUI do cliente de backup-archive, clique em **Utilitários** > **Assistente de Configuração** > **Ajude-me a configurar o Client Scheduler**. Clique em **Avançar**.
2. Leia as informações na página Assistente do planejador e clique em **Avançar**.
3. Na página Tarefa do planejador, selecione **Instalar um planejador novo ou adicional** e clique em **Avançar**.
4. No Nome e localização do planejador, especifique um nome para o planejador de cliente que você está incluindo. Em seguida, selecione **Usar o Client Acceptor daemon (CAD)** para gerenciar o planejador e clique em **Avançar**.
5. Insira o nome que deseja designar a esse client acceptor. O nome padrão é Client Acceptor. Clique em **Avançar**.
6. Conclua a configuração percorrendo o assistente.
7. Atualize o arquivo de opções do cliente, `dsm.opt`, e configure a opção **`passwordaccess`** como `generate`.
8. Para armazenar a senha de nó do cliente, emita o seguinte comando no prompt de comandos:

   ```
   dsmc query sess
   ```

   Insira a senha de nó do cliente quando solicitado.
9. Inicie o serviço do client acceptor a partir da página Controle de serviços. Por exemplo, se você usou o nome padrão, inicie o serviço do Client Acceptor. Não inicie o serviço do planejador que você especificou na página Nome e Local do Planejador. O serviço do planejador é iniciado e interrompido automaticamente pelo serviço de client acceptor conforme necessário.

Configurando as comunicações entre o servidor e o cliente por meio de um firewall

Se um cliente precisar se comunicar com um servidor por meio de um firewall, deve-se ativar as comunicações entre o servidor e o cliente por meio do firewall.

Antes de Iniciar

Se você usou o assistente Incluir Cliente para registrar um cliente, localize os valores de opção no arquivo de opções do cliente que você obteve durante esse processo. É possível usar valores para especificar portas.

Sobre Esta Tarefa

Atenção: Não configure um firewall de uma maneira que possa causar o término de sessões que estão em uso por um servidor ou agente de armazenamento. O término de uma sessão válida pode causar resultados imprevisíveis. Os processos e sessões podem parecer parar devido a erros de entrada/saída. Para ajudar a excluir sessões de restrições de tempo limite, configure as portas conhecidas para componentes do IBM Spectrum Protect. Certifique-se de que a opção do servidor **KEEPALIVE** permaneça configurada como o valor padrão de YES. Dessa forma, é possível ajudar a assegurar que a comunicação entre o servidor e o cliente seja ininterrupta. Para obter instruções sobre como configurar a opção do servidor **KEEPALIVE**, consulte KEEPALIVE.

Procedimento

Abra as seguintes portas para permitir acesso pelo firewall:

Porta TCP/IP para o cliente de backup-archive, o cliente administrador da linha de comandos e o planejador de cliente
Especifique a porta usando a opção **tcpport** no arquivo de opções do cliente. A opção **tcpport** no arquivo de opções do cliente deve corresponder à opção **TCPPORT** no arquivo de opções do servidor. O valor padrão é 1500. Se você decidir usar um valor diferente do padrão, especifique um número no intervalo de 1024 a 32767.

Porta HTTP para ativar a comunicação entre o Web client e estações de trabalho remotas
Especifique a porta para a estação de trabalho remota configurando a opção **httpport** no arquivo de opções do cliente da estação de trabalho remota. O valor padrão é 1581.

Portas TCP/IP para a estação de trabalho remota
O valor padrão de 0 (zero) faz com que dois números de portas livres sejam designados aleatoriamente à estação de trabalho remota. Se não desejar que os números de portas sejam designados aleatoriamente, especifique valores configurando a opção **webports** no arquivo de opções do cliente da estação de trabalho remota.

Porta TCP/IP para sessões administrativas
Especifique a porta na qual o servidor espera solicitações para sessões administrativas do cliente. O valor da opção **tcpadminport** do cliente deve corresponder ao valor da opção do servidor **TCPADMINPORT**. Dessa forma, é possível proteger sessões administrativas em uma rede privada.

Gerenciando operações do cliente

É possível avaliar e resolver erros relacionados a um cliente de backup-archive usando o Operations Center, que fornece sugestões para resolver erros. Para erros em outros tipos de clientes, deve-se examinar os logs de erros no cliente e revisar a documentação do produto.

Sobre Esta Tarefa

Em alguns casos, é possível resolver erros do cliente parando e iniciando o client acceptor. Se os nós clientes ou IDs de administrador estiverem bloqueados, será possível resolver o problema desbloqueando o nó cliente ou o ID de administrador e, em seguida, reconfigurando a senha.

Para obter instruções detalhadas sobre como identificar e resolver erros de clientes, consulte Resolvendo problemas do cliente.

Avaliando erros nos logs de erros do cliente

É possível resolver erros do cliente obtendo sugestões do Operations Center ou revisando os logs de erro no cliente.

Antes de Iniciar

Para resolver erros em um cliente de backup-archive em um sistema operacional Linux ou Windows, certifique-se de que o client management service esteja instalado e iniciado. Para obter instruções de instalação, consulte "Instalando o serviço de gerenciamento de clientes" na página 70. Para obter instruções sobre como verificar a instalação, consulte "Verificando que o serviço de gerenciamento de clientes está instalado corretamente" na página 71.

Procedimento

Para diagnosticar e resolver erros do cliente, execute uma das seguintes ações:

- Se o client management service estiver instalado no nó cliente, conclua as etapas a seguir:
  1. Na página Visão geral do Operations Center, clique em **Clientes** e selecione o cliente.
  2. Clique em **Detalhes**.
  3. Na página Resumo do cliente, clique na guia **Diagnóstico**.
  4. Revise as mensagens de log recuperadas.

     Dicas:
     - Para mostrar ou ocultar a área de janela Logs do cliente, dê clique duplo na barra Logs do cliente.
     - Para redimensionar a área de janela Logs do cliente, clique e arraste a barra Logs do cliente.

     Se forem exibidas sugestões na página Diagnóstico, selecione uma sugestão. Na área de janela Logs do cliente, as mensagens de log do cliente às quais a sugestão está relacionada são destacadas.
  5. Use as sugestões para resolver os problemas indicados pelas mensagens de erro.

     Dica: Sugestões são fornecidas apenas para um subconjunto de mensagens do cliente.
- Se o client management service não estiver instalado no nó cliente, revise os logs de erro para o cliente instalado.

Parando e reiniciando o client acceptor

Se você mudar a configuração de sua solução, deverá reiniciar o client acceptor em todos os nós clientes em que um cliente de backup-archive está instalado.

Sobre Esta Tarefa

Em alguns casos, é possível resolver problemas de planejamento de cliente parando e reiniciando o client acceptor. O client acceptor deve estar em execução para assegurar que as operações planejadas possam ocorrer no cliente. Por exemplo, se você mudar o endereço IP ou nome de domínio do servidor, deverá reiniciar o client acceptor.

Procedimento

Siga as instruções para o sistema operacional que está instalado no nó cliente:

AIX e Oracle Solaris

- Para parar o client acceptor, conclua as etapas a seguir:
  1. Determine o ID do processo para o client acceptor, emitindo o comando a seguir na linha de comandos:

     ```
     ps -ef | grep dsmcad
     ```

     Revise a saída. Na saída de amostra a seguir, 6764 é o ID do processo para o client acceptor:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```
  2. Emita o seguinte comando na linha de comandos:

     ```
     kill -9 PID
     ```

     em que *PID* especifica o ID do processo para o client acceptor.
- Para iniciar o client acceptor, emita o comando a seguir na linha de comandos:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Para parar o client acceptor (e não reiniciá-lo), emita o comando a seguir:

  ```
  # service dsmcad stop
  ```
- Para parar e reiniciar o client acceptor, emita o comando a seguir:

  ```
  # service dsmcad restart
  ```

MAC OS X

Clique em **Aplicativos** > **Utilitários** > **Terminal**.

- Para parar o client acceptor, emita o comando a seguir:

  ```
  /bin/launchctl unload -w com.ibm.tivoli.dsmcad
  ```
- Para iniciar o client acceptor, emita o comando a seguir:

  ```
  /bin/launchctl load -w com.ibm.tivoli.dsmcad
  ```

Windows

- Para parar o serviço de client acceptor, conclua as etapas a seguir:
  1. Clique em **Iniciar** > **Ferramentas administrativas** > **Serviços**.
  2. Clique duas vezes no serviço de client acceptor.
  3. Clique em **Parar** e em **OK**.

- Para reiniciar o serviço de client acceptor, conclua as etapas a seguir:
  1. Clique em **Iniciar** > **Ferramentas administrativas** > **Serviços**.
  2. Clique duas vezes no serviço de client acceptor.
  3. Clique em **Iniciar** e em **OK**.

Referências relacionadas:

Resolvendo Problemas de Planejamento de Cliente

Reconfigurando senhas

Se uma senha para um nó cliente ou um ID de administrador for perdida ou esquecida, será possível reconfigurar a senha. Várias tentativas de acessar o sistema com uma senha incorreta podem causar bloqueio de um nó cliente ou de um ID de administrador. É possível executar etapas para resolver o problema.

Procedimento

Para resolver problemas de senha, execute uma das seguintes ações:

- Se um cliente de backup-archive estiver instalado em um nó cliente, e a senha for perdida ou esquecida, conclua as etapas a seguir:
  1. Gere uma nova senha emitindo o comando **UPDATE NODE**:

     ```
     update node node_name new_password forcepwreset=yes
     ```

     em que *node_name* especifica o nó cliente e *new_password* especifica a senha designada.
  2. Informe o proprietário do nó cliente sobre a senha alterada. Quando o proprietário do nó cliente efetuar login com a senha especificada, uma nova senha será gerada automaticamente. Essa senha é desconhecida para os usuários para aprimorar a segurança.

     Dica: A senha será gerada automaticamente se você configurou anteriormente a opção **passwordaccess** como `generate` no arquivo de opções do cliente.
- Se um administrador estiver bloqueado devido a problemas de senha, conclua as etapas a seguir:
  1. Para fornecer ao administrador acesso ao servidor, emita o comando **UNLOCK ADMIN**. Para obter instruções, consulte UNLOCK ADMIN (Desbloquear um Administrador).
  2. Configure uma nova senha usando o comando **UPDATE ADMIN**:

     ```
     update admin admin_name new_password forcepwreset=yes
     ```

     em que *admin_name* especifica o nome do administrador e *new_password* especifica a senha designada.
- Se um nó cliente estiver bloqueado, conclua as etapas a seguir:
  1. Determine por que o nó cliente está bloqueado e se ele deve ser desbloqueado. Por exemplo, se o nó cliente for desatribuído, ele está sendo removido do ambiente de produção. Não é possível reverter a operação de desatribuição, e o nó cliente permanece bloqueado. Um nó cliente também pode ser bloqueado se os dados de cliente forem o assunto de uma investigação judicial.
  2. Se precisar desbloquear um nó cliente, use o comando **UNLOCK NODE**. Para obter instruções, consulte UNLOCK NODE (Desbloquear um nó de cliente).
  3. Gere uma nova senha emitindo o comando **UPDATE NODE**:

```
update node node_name new_password forcepwreset=yes
```

em que *node_name* especifica o nome do nó e *new_password* especifica a senha designada.

4. Informe o proprietário do nó cliente sobre a senha alterada. Quando o proprietário do nó cliente efetuar login com a senha especificada, uma nova senha será gerada automaticamente. Essa senha é desconhecida para os usuários para aprimorar a segurança.

   Dica: A senha será gerada automaticamente se você configurou anteriormente a opção **passwordaccess** como `generate` no arquivo de opções do cliente.

Modificando o escopo de um backup de cliente

Ao configurar operações de backup do cliente, a prática preferencial é excluir objetos desnecessários. Por exemplo, geralmente você deseja excluir arquivos temporários de uma operação de backup.

Sobre Esta Tarefa

Ao excluir objetos desnecessários de operações de backup, você obtém melhor controle da quantidade de espaço de armazenamento necessário para operações de backup e do custo de armazenamento. Dependendo de seu pacote de licenciamento, também é possível limitar custos de licenciamento.

Procedimento

Como você modifica o escopo de operações de backup depende do produto que está instalado no nó cliente:

- Para um cliente de backup-archive, é possível criar uma lista de inclusão/exclusão para incluir ou excluir um arquivo, grupos de arquivos ou diretórios de operações de backup. Para criar uma lista de inclusão/exclusão, siga as instruções em Criando uma Lista de Inclusão-Exclusão.

  Para assegurar o uso consistente de uma lista de inclusão/exclusão para todos os clientes de um tipo, é possível criar um conjunto de opções do cliente no servidor que contenha as opções necessárias. Em seguida, designe o conjunto de opções do cliente a cada um dos clientes do mesmo tipo. Para obter detalhes, consulte a seção Controlando operações do cliente através dos conjuntos de opções do cliente.
- Para um cliente de backup-archive, é possível especificar os objetos a serem incluídos em uma operação de backup incremental usando a opção **domain**. Siga as instruções em Opção de domínio.
- Para outros produtos, para definir quais objetos são incluídos em e excluídos das operações de backup, siga as instruções na documentação do produto.

Gerenciando upgrades do cliente

Quando um fix pack ou correção temporária se torna disponível para um cliente, é possível fazer upgrade do cliente para tirar vantagem das melhorias do produto. Os servidores e clientes podem ser atualizados em diferentes horários e podem estar em diferentes níveis com algumas restrições.

Antes de Iniciar

1. Revise os requisitos de compatibilidade do cliente/servidor em nota técnica 1053218. Se sua solução incluir servidores ou clientes em um nível anterior à V7.1, revise as diretrizes para assegurar que as operações de backup e archive do cliente não sejam interrompidas.
2. Verifique os requisitos do sistema para o cliente em Sistemas Operacionais Suportados do IBM Spectrum Protect.
3. Se a solução incluir agentes de armazenamento ou clientes de biblioteca, revise as informações sobre compatibilidade de agente de armazenamento e cliente de biblioteca com servidores que estão configurados como gerenciadores de biblioteca. Consulte nota técnica 1302789.

   Se você planeja fazer upgrade de um gerenciador de biblioteca e de um cliente de biblioteca, deve-se fazer upgrade do gerenciador de biblioteca primeiro.

Procedimento

Para fazer upgrade do software, conclua as instruções que estão listadas na tabela a seguir.

Software	Link para instruções
Cliente de backup-archive do IBM Spectrum Protect	• Planejando atualizações do cliente
IBM Spectrum Protect Snapshot	• Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para UNIX e Linux • Instalando e fazendo upgrade do IBM Spectrum Protect Snapshot para VMware • Instalando e Atualizando o IBM Spectrum Protect Snapshot para Windows
IBM Spectrum Protect for Databases	• Atualizando o Data Protection for SQL Server • Instalação do Data Protection for Oracle • Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Fazendo upgrade do IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Db2 • Fazendo upgrade do IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Instalação do Data Protection for IBM Domino em um sistema UNIX, AIX ou Linux (V7.1.0) • Instalação do Data Protection for IBM Domino em um sistema Windows (V7.1.0) • Instalando, fazendo upgrade e migrando o IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Instalando e Atualizando o Proteção de Dados para VMware • Instalando o Data Protection for Microsoft Hyper-V

Desatribuindo um nó cliente

Se um nó cliente não for mais necessário, será possível iniciar um processo para removê-lo do ambiente de produção. Por exemplo, se uma estação de trabalho estava fazendo backup dos dados para o servidor IBM Spectrum Protect, mas ela não for mais usada, será possível desatribuir a estação de trabalho.

Sobre Esta Tarefa

Ao iniciar o processo de desatribuição, o servidor bloqueia o nó cliente para evitar que ele acesse o servidor. Os arquivos que pertencem ao nó cliente são excluídos gradualmente e, em seguida, o nó cliente é excluído. É possível desatribuir os seguintes tipos de nós clientes:

Nós clientes do aplicativo
Os nós clientes do aplicativo incluem servidores de e-mail, bancos de dados e outros aplicativos. Por exemplo, qualquer um dos seguintes aplicativos pode ser um nó cliente do aplicativo:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nós clientes do sistema
Os nós clientes do sistema incluem estações de trabalho, servidores de arquivos de armazenamento conectado à rede (NAS) e clientes da API.

Nós clientes de máquina virtual
Os nós clientes de máquina virtual consistem em um host convidado individual em um hypervisor. Cada máquina virtual é representada como um espaço no arquivo.

Restrição: Não é possível desatribuir um nó cliente de objeto.

O método mais simples para desatribuir um nó cliente é usar o Operations Center. O processo de desatribuição é executado no segundo plano. Se o cliente estiver configurado para replicar dados de cliente, o Operations Center removerá automaticamente o cliente da replicação nos servidores de replicação de origem e de destino antes de desatribuir o cliente.

Dica: Como alternativa, é possível desatribuir um nó cliente emitindo o comando **DECOMMISSION NODE** ou **DECOMMISSION VM**. Talvez você queira usar esse método nos seguintes casos:

- Para planejar o processo de desatribuição para o futuro ou para executar uma série de comandos usando um script, especifique o processo de desatribuição para execução no segundo plano.
- Para monitorar o processo de desatribuição para propósitos de depuração, especifique o processo de desatribuição para execução no primeiro plano. Se você executar o processo no primeiro plano, deverá aguardar a conclusão do processo antes de continuar com outras tarefas.

Procedimento

Execute uma das seguintes ações:

- Para desatribuir um cliente no segundo plano usando o Operations Center, conclua as etapas a seguir:
  1. Na página Visão geral do Operations Center, clique em **Clientes** e selecione o cliente.
  2. Clique em **Mais** > **Desatribuir**.
- Para desatribuir um nó cliente usando um comando administrativo, conclua as etapas a seguir:
  1. Determine se o nó cliente está configurado para replicação de nó emitindo o comando **QUERY NODE**. Por exemplo, se o nó cliente chamar-se AUSTIN, execute o seguinte comando:

     ```
     query node austin format=detailed
     ```

     Revise o campo de saída **Estado de Replicação**.
  2. Se o nó cliente estiver configurado para replicação, remova-o da replicação emitindo o comando **REMOVE REPLNODE**. Por exemplo, se o nó cliente chamar-se AUSTIN, emita o seguinte comando:

     ```
     remove replnode austin
     ```
  3. Execute uma das seguintes ações:
     - Para desatribuir um nó cliente do aplicativo ou do sistema no segundo plano, emita o comando **DECOMMISSION NODE**. Por exemplo, se o nó cliente chamar-se AUSTIN, emita o seguinte comando:

       ```
       decommission node austin
       ```
     - Para desatribuir um nó cliente do aplicativo ou do sistema no primeiro plano, emita o comando **DECOMMISSION NODE** e especifique o parâmetro `wait=yes`. Por exemplo, se o nó cliente chamar-se AUSTIN, emita o seguinte comando:

       ```
       decommission node austin wait=yes
       ```
     - Para desatribuir uma máquina virtual no segundo plano, emita o comando **DECOMMISSION VM**. Por exemplo, se a máquina virtual chamar-se AUSTIN, o espaço no arquivo for 7 e o nome do espaço no arquivo for especificado pelo ID do espaço no arquivo, emita o seguinte comando:

       ```
       decommission vm austin 7 nametype=fsid
       ```

       Se o nome da máquina virtual incluir um ou mais espaços, coloque-o entre aspas duplas. Por exemplo:

       ```
       decommission vm "austin 2" 7 nametype=fsid
       ```
     - Para desatribuir uma máquina virtual no primeiro plano, emita o comando **DECOMMISSION VM** e especifique o parâmetro `wait=yes`. Por exemplo, emita o seguinte comando:

       ```
       decommission vm austin 7 nametype=fsid wait=yes
       ```

       Se o nome da máquina virtual incluir um ou mais espaços, coloque-o entre aspas duplas. Por exemplo:

       ```
       decommission vm "austin 2" 7 nametype=fsid wait=yes
       ```

O que Fazer Depois

Fique atento às mensagens de erro, que podem ser exibidas na interface com o usuário ou na saída de comando, imediatamente após a execução do processo.

É possível verificar se o nó cliente está desatribuído:

1. Na página Visão geral do Operations Center, clique em **Clientes**.
2. Na tabela Clientes, na coluna Em risco, revise o estado:

- Um estado DECOMMISSIONED especifica que o nó está desatribuído.
- Um valor nulo especifica que o nó não está desatribuído.
- Um estado PENDING especifica que o nó está sendo desatribuído ou que o processo de desatribuição falhou.

Dica: Se quiser determinar o status de um processo de desatribuição pendente, emita o seguinte comando:

```
query process
```

3. Revise a saída de comando:
   - Caso um status seja fornecido para o processo de desatribuição, o processo está em andamento. Por exemplo:

```
query process

 Process     Process Description           Process Status
  Number
--------     --------------------     -----------------------------------------
       3          DECOMMISSION NODE        Number of backup objects deactivated
                                           for node NODE1: 8 objects deactivated.
```

   - Caso nenhum status seja fornecido para o processo de desatribuição e você não receber uma mensagem de erro, o processo está incompleto. Um processo pode estar incompleto caso os arquivos que estão associados ao nó ainda não tenham sido desativados. Após a desativação dos arquivos, execute o processo de desatribuição novamente.
   - Caso nenhum status seja fornecido para o processo de desatribuição e você receber uma mensagem de erro, o processo falhou. Execute o processo de desatribuição novamente.

Referências relacionadas:

- DECOMMISSION NODE (Desatribuir um nó cliente)
- DECOMMISSION VM (Desatribuir uma máquina virtual)
- QUERY NODE (Consultar nós)
- REMOVE REPLNODE (Remover um nó cliente da replicação)

Desativando dados para liberar espaço de armazenamento

Em alguns casos, é possível desativar os dados que são armazenados no servidor IBM Spectrum Protect. Ao executar o processo de desativação, os dados de backup que foram armazenados antes da data e hora especificadas serão desativados e excluídos conforme expiram. Dessa forma, é possível liberar espaço no servidor.

Sobre Esta Tarefa

Alguns aplicativos clientes sempre salvam dados no servidor como dados de backup ativo. Como os dados de backup ativo não são gerenciados por políticas de expiração de inventário, os dados não são excluídos automaticamente e usam o espaço de armazenamento do servidor indefinidamente. Para liberar o espaço de armazenamento que é usado por dados obsoletos, é possível desativar os dados.

Ao executar o processo de desativação, todos os dados de backup ativo que foram armazenados antes da data especificada se tornam inativos. Os dados são excluídos conforme expiram e não podem ser restaurados. O recurso de desativação aplica-se apenas aos aplicativos clientes que protegem bancos de dados Oracle.

Procedimento

1. Na página Visão geral do Operations Center, clique em **Clientes**.
2. Na tabela Clientes, selecione um ou mais clientes e clique em **Mais** > **Limpar**.

Método de linha de comandos: Desative os dados usando o comando **DEACTIVATE DATA**.

Referências relacionadas:

DEACTIVATE DATA (Desativar dados para um nó cliente)

Capítulo 19. Gerenciando armazenamento de dados

Gerencie seus dados para eficiência e inclua dispositivos suportados e mídia no servidor para armazenar os dados do cliente.

Referências relacionadas:

Tipos de conjuntos de armazenamentos

Auditando um contêiner do conjunto de armazenamentos

Faça a auditoria de um contêiner de conjunto de armazenamentos para verificar inconsistências entre as informações do banco de dados e um contêiner em um conjunto de armazenamentos.

Sobre Esta Tarefa

Audite um contêiner do conjunto de armazenamentos nas seguintes situações:

- Ao emitir o comando **QUERY DAMAGED** e for detectado um problema
- Se o servidor exibir mensagens sobre extensões de dados danificadas
- Seu hardware relatar um problema e forem exibidas mensagens de erro que estão associadas ao contêiner do conjunto de armazenamentos.

Procedimento

1. Para auditar um contêiner do conjunto de armazenamentos, emita o comando **AUDIT CONTAINER**. Por exemplo, emita o seguinte comando para auditar um contêiner, `000000000000076c.dcf`:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Revise a saída da mensagem ANR4891I para informações sobre extensões de dados danificadas.

O que Fazer Depois

Se você detectar problemas com o contêiner do conjunto de armazenamentos, será possível restaurar dados com base em sua configuração. É possível reparar os conteúdos no conjunto de armazenamentos usando o comando **REPAIR STGPOOL**.

Restrição: Só é possível reparar os conteúdos do conjunto de armazenamentos se você protegeu o conjunto de armazenamentos usando o comando **PROTECT STGPOOL**.

Referências relacionadas:

AUDIT CONTAINER (Verificar a consistência de informações do banco de dados para um conjunto de armazenamentos de contêineres de diretório)

QUERY DAMAGED (Consultar dados danificados em um conjunto de armazenamentos de contêiner em nuvem ou de contêiner-diretório)

Gerenciando a capacidade do inventário

Gerencie a capacidade do banco de dados, do log ativo e dos logs de archive para assegurar que o inventário seja dimensionado para as tarefas, com base no status dos logs.

Antes de Iniciar

Os logs ativos e de archive possuem as seguintes características:

- O log ativo pode ter um tamanho máximo de 512 GB. Para obter mais informações sobre o dimensionamento do log ativo para o seu sistema, consulte Planejando as matrizes de armazenamento.
- O tamanho do log de archive é limitado ao tamanho do sistema de arquivos no qual está instalado. O tamanho do log de archive não é mantido em um tamanho predefinido, como o log ativo. Os arquivos de log de archive são excluídos automaticamente quando não são mais necessários.

Como uma melhor prática, opcionalmente, é possível criar um log de failover de archive para armazenar arquivos de log de archive quando o diretório de log de archive estiver cheio.

Verifique o Operations Center para determinar o componente do inventário que está cheio. Certifique-se de parar o servidor antes de aumentar o tamanho de um dos componentes do inventário.

Procedimento

- Para aumentar o tamanho do banco de dados, conclua as etapas a seguir:
  - Crie um ou mais diretórios para o banco de dados em unidades ou sistemas de arquivos separados.
  - Emita o comando **EXTEND DBSPACE** para incluir o diretório ou diretórios no banco de dados. Os diretórios devem estar acessíveis ao ID do usuário da instância do gerenciador do banco de dados. Por padrão, os dados são redistribuídos entre todos os diretórios do banco de dados e o espaço é recuperado.

    Dicas:

    - O tempo necessário para concluir a redistribuição de dados e a recuperação de espaço é variável, dependendo do tamanho de seu banco de dados. Certifique-se de planejar de forma apropriada.
    - Assegure-se de que os diretórios especificados sejam do mesmo tamanho que os diretórios existentes, para assegurar um grau de paralelismo consistente para operações de banco de dados. Se um ou mais diretórios do banco de dados forem menores que os outros, eles reduzirão o potencial de pré-busca e distribuição paralela otimizada do banco de dados.
  - Pare e reinicie o servidor para usar totalmente os novos diretórios.
  - Reorganize o banco de dados, se necessário. A reorganização de índice e de tabela para o banco de dados do servidor pode ajudar a evitar o crescimento inesperado do banco de dados e problemas de desempenho. Para obter informações adicionais sobre a reorganização do banco de dados, consulte nota técnica 1683633.
- Para diminuir o tamanho do banco de dados para os servidores V7.1 e mais recentes, emita os seguintes comandos do IBM Db2 do diretório de instância do servidor:

Restrição: Os comandos podem aumentar a atividade de E/S e podem afetar o desempenho do servidor. Para minimizar problemas de desempenho, aguarde até que um comando seja concluído antes de emitir o próximo comando. Os comandos do Db2 podem ser emitidos durante a execução do servidor.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- Para aumentar ou diminuir o tamanho do log ativo, conclua as etapas a seguir:
  1. Certifique-se de que o local do log ativo tenha espaço suficiente para o tamanho de log aumentado. Se existir um espelho de log, seu local também deverá ter espaço suficiente para o tamanho do log aumentado.
  2. Pare o servidor.
  3. No arquivo `dsmserv.opt`, atualize a opção **`ACTIVELOGSIZE`** para o novo tamanho do log ativo, em megabytes.

     O tamanho de um arquivo de log ativo é baseado no valor da opção `ACTIVELOGSIZE`. As diretrizes para requisitos de espaço estão na seguinte tabela:

Tabela 17. Como estimar requisitos de volume e de espaço no arquivo

Valor da opção `ACTIVELOGSize`	**Reserve essa quantidade de espaço livre no diretório de log ativo, além do espaço `ACTIVELOGSize`**
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

     Para alterar o log ativo para seu tamanho máximo de 512 GB, insira a seguinte opção do servidor:

     ```
     activelogsize 524288
     ```

  4. Se você planeja usar um novo diretório de log ativo, atualize o nome do diretório especificado na opção do servidor **`ACTIVELOGDIRECTORY`**. O novo diretório deve estar vazio e deve estar acessível para o ID do usuário do gerenciador do banco de dados.
  5. Reinicie o servidor.

- Compacte os logs de archive para reduzir a quantidade de espaço necessário para armazenamento. Ative a compactação dinâmica do log de archive emitindo o seguinte comando:

  ```
  setopt archlogcompress yes
  ```

  Restrição: Tenha cuidado ao ativar a opção do servidor **ARCHLOGCOMPRESS** em sistemas com alto uso de volumes sustentados e cargas de trabalho pesadas. A ativação dessa opção neste ambiente do sistema pode causar atrasos no arquivamento de arquivos de log do sistema de arquivos de log ativo para o sistema de arquivos de log de archive. Este atraso pode fazer com que o sistema de arquivos de log ativo fique sem espaço. Certifique-se de monitorar o espaço disponível no sistema de arquivos de log ativo após a compactação do log de archive ser ativada. Se o uso do sistema de arquivos do diretório de log ativo se aproximar de condições de falta de espaço, a opção do servidor **ARCHLOGCOMPRESS** deve ser desativada. É possível usar o comando **SETOPT** para desativar a compactação de log de archive imediatamente sem parar o servidor.

Referências relacionadas:

- Opção do servidor ACTIVELOGSIZE
- EXTEND DBSPACE (Aumentar o Espaço do Banco de Dados)
- SETOPT (Definir uma opção do servidor para atualização dinâmica)

Gerenciando o uso de memória e de processor

Assegure-se de gerenciar os requisitos de memória e uso do processador para garantir que o servidor possa concluir os processos de dados como backup e deduplicação de dados. Considere o impacto no desempenho quando concluir determinados processos.

Antes de Iniciar

- Certifique-se de que sua configuração use os requisitos de hardware e de software. Para obter informações adicionais, consulte Sistemas Operacionais Suportados do IBM Spectrum Protect.
- Para obter informações adicionais sobre como gerenciar recursos, como o banco de dados e o log de recuperação, consulte Planejando as matrizes de armazenamento.
- Inclua mais memória do sistema para determinar se há uma melhoria de desempenho. Monitore o uso de memória regularmente para determinar se mais memória é necessária.

Procedimento

1. Libere memória do cache do sistema de arquivos, onde for possível.
2. Para gerenciar a memória do sistema que é usada por cada servidor em um sistema, use a opção do servidor `DBMEMPERCENT`. Limite a porcentagem de memória do sistema que pode ser usada pelo gerenciador do banco de dados de cada servidor. Se todos os servidores forem igualmente importantes, utilize o mesmo valor para cada servidor. Se um servidor for o servidor de produção e os outros servidores forem servidores de teste, configure o valor para o servidor de produção para um valor mais alto que dos servidores de teste.
3. Configure o limite de dados do usuário e memória privada para o banco de dados para assegurar que memória privada não esteja esgotada. O esgotamento da memória privada pode resultar em erros, menos desempenho ideal e instabilidade.

Ajustando atividades planejadas

Planeje tarefas de manutenção diariamente para assegurar que sua solução funcione corretamente. Ao ajustar sua solução, você maximiza os recursos do servidor e usa efetivamente diferentes funções disponíveis em sua solução.

Procedimento

1. Monitore o desempenho do sistema regularmente para assegurar que tarefas de backup de cliente e de manutenção de servidor sejam concluídas com sucesso. Siga as instruções em Parte 3, "Monitorando uma solução de disco multisite", na página 81.
2. Opcional: Se as informações de monitoramento mostrarem que houve aumento da carga de trabalho do servidor, revise as informações de planejamento. Revise se a capacidade do sistema é adequada nos seguintes casos:
   - O número de clientes aumentou
   - A quantidade de dados que está sendo feito backup aumentou
   - A quantidade de tempo que está disponível para backups foi alterada
3. Determine se sua solução está tendo um desempenho no nível esperado. Revise os planejamentos de cliente para verificar se as tarefas estão sendo concluídas dentro do prazo planejado:
   a. Na página **Clientes** do Operations Center, selecione o cliente.
   b. Clique em **Detalhes**.
   c. Na página Resumo do cliente, revise as atividades **Backup Realizado** e **Replicados** para identificar quaisquer riscos.

   Ajuste o tempo e a frequência de operações de backup de cliente, se necessário.
4. Planeje tempo suficiente para que as seguintes tarefas de manutenção sejam concluídas com sucesso dentro de um período de 24 horas:
   a. Proteger conjuntos de armazenamentos.
   b. Replicar dados do nó.
   c. Faça backup do banco de dados.
   d. Executar o processo de expiração para remover backups de cliente e cópias de archive do armazenamento do servidor.

   Dica: Planeje tarefas de manutenção para iniciar em um horário apropriado e na sequência correta. Por exemplo, planeje tarefas de replicação após a conclusão bem-sucedida de backups de cliente.

Conceitos relacionados:

Desempenho

Tarefas relacionadas:

Deduplicando dados (V7.1.1)

"Definindo planejamentos para atividades de manutenção de servidor" na página 66

Movendo clientes de um servidor para outro

Para evitar ficar sem espaço em um servidor ou para resolver problemas de carga de trabalho, você pode ter que mover nós clientes de um servidor para outro.

Antes de Iniciar

Planeje a capacidade para sua solução para assegurar que haja espaço suficiente para nós clientes no servidor, que inclui espaço para crescimento futuro.

Sobre Esta Tarefa

Ao mover os nós clientes, é possível deixar seus backups existentes no servidor original para expirarem de acordo com sua política de expiração, ou exportar seus backups existentes para o novo servidor.

Procedimento

Conclua as etapas a seguir para mover um nó cliente para outro servidor.

1. Exporte o nó cliente diretamente para um novo servidor usando o comando **EXPORT NODE**.
2. Atualize o arquivo de opções do cliente com o nome do novo servidor.
3. No novo servidor, designe um planejamento para o nó cliente para fazer backup dos dados.
   a. Na página **Clientes** do Operations Center, selecione o nó cliente.
   b. Clique em **Mais** > **Associação de planejamento**.
   c. Selecione a caixa de seleção nas linhas de planejamento às quais você deseja designar o nó cliente selecionado.
   d. Clique em **Salvar**.
4. Emita novamente o comando **EXPORT NODE** para exportar dados de forma incremental do servidor original para o novo servidor. Ao exportar dados de forma incremental, você exporta dados que foram submetidos a backup entre o primeiro processo de exportação e quando foi designado um planejamento ao nó cliente.
5. Monitore o nó cliente para assegurar que ele esteja fazendo backup de dados, de acordo com o planejamento configurado e para monitorar se o nó cliente está em risco. Passe o mouse sobre **Clientes** e clique em **Planejamentos**.
6. Desatribua o nó cliente do servidor original concluindo as etapas a seguir.
   a. Na página **Visão geral** do Operations Center, clique em **Clientes**.
   b. Na tabela Clientes, selecione o nó cliente.
   c. Clique em **Mais** > **Desatribuir**.

   O nó cliente é removido do servidor original. À medida que os dados expiram, conforme especificado em suas configurações de política, os dados do nó cliente são excluídos. Após a exclusão dos dados do nó cliente, o cliente é removido do servidor.

Referências relacionadas:

EXPORT NODE (Exportar informações do nó de cliente)

IMPORT NODE (Importar informações do nó de cliente)

Capítulo 20. Gerenciando a replicação

Use a replicação para recuperar dados em um site de recuperação de desastre e manter os mesmos níveis de arquivos nos servidores de origem e de destino. É possível gerenciar a replicação no nível do nó. Também é possível proteger dados no nível de conjunto de armazenamentos.

Compatibilidade de replicação

Antes de configurar operações de replicação com o IBM Spectrum Protect, deve-se assegurar que os servidores de replicação de origem e de destino sejam compatíveis para replicação.

Tabela 18. Compatibilidade de replicação de versões do servidor

Versão do servidor de replicação de origem	Versões compatíveis para o servidor de replicação de destino
V7.1	V7.1 ou mais recente
V7.1.1	V7.1 ou mais recente
V7.1.3	V7.1.3 ou posterior
V7.1.4	V7.1.3 ou posterior
V7.1.5	V7.1.3 ou posterior
V7.1.6	V7.1.3 ou posterior
V7.1.7	V7.1.3 ou posterior
V7.1.8	V7.1.3 ou posterior
V8.1	V7.1.3 ou posterior
V8.1.1	V7.1.3 ou posterior
Versão 8.1.2	V7.1.3 ou posterior
V8.1.3	V7.1.3 ou posterior
V8.1.4	V7.1.3 ou posterior
V8.1.5	V7.1.3 ou posterior
V8.1.6	V7.1.3 ou posterior
V8.1.7	V7.1.3 ou posterior

Ativando a replicação de nó

É possível ativar a replicação de nó para proteger seus dados.

Antes de Iniciar

Assegure-se de que os servidores de origem e de destino sejam compatíveis para replicação.

Sobre Esta Tarefa

Replique o nó cliente para replicar todos os dados de cliente, incluindo metadados. Por padrão, a replicação de nó é desativada ao iniciar o servidor pela primeira vez.

Dicas:

- Para reduzir o tempo de processamento de replicação, proteja o conjunto de armazenamentos antes de replicar os nós clientes. Quando a replicação de nó é iniciada, as extensões de dados que já são replicadas por meio da proteção de conjunto de armazenamentos são ignoradas.
- A replicação requer quantias maiores de memória e largura da banda suficiente para concluir o processamento. Dimensione o banco de dados e seus logs para assegurar que as transações possam ser concluídas.

Procedimento

Para ativar a replicação de nó, conclua as etapas a seguir no Operations Center:

1. Na página Servidores, clique em **Detalhes**.
2. Na página Detalhes, clique em **Propriedades**.
3. Na seção **Replicação**, selecione **Ativado** no campo **Replicação de saída**.
4. Clique em **Salvar**.

O que Fazer Depois

Conclua as seguintes ações:

1. Para verificar se a replicação foi bem-sucedida, revise o Capítulo 13, “Lista de verificação de monitoramento diária”, na página 83.
2. Linux Se o servidor IBM Spectrum Protect replicar nós para um servidor remoto, determine se a tecnologia Aspera Fast Adaptive Secure Protocol (FASP) pode melhorar o rendimento de dados para o servidor remoto. Siga as instruções em Determinando se a tecnologia Aspera FASP pode otimizar a transferência de dados em seu ambiente de sistema.

Referências relacionadas:

“Compatibilidade de replicação” na página 143

Protegendo dados em conjuntos de armazenamentos de contêiner de diretório

Proteja os dados em conjunto de armazenamentos de contêiner de diretório para reduzir o tempo de replicação de nó e permitir o reparo dos dados em conjuntos de armazenamentos de contêiner de diretório.

Antes de Iniciar

Assegure-se de que pelo menos um conjunto de armazenamentos de contêiner-diretório exista no servidor de replicação de destino. Ao ativar a replicação no Operations Center, é possível planejar a proteção do conjunto de armazenamentos. Para configurar a replicação e ativar a proteção do conjunto de armazenamentos, conclua as seguintes etapas:

1. Na barra de menus do Operations Center, passe o mouse sobre **Armazenamento** e clique em **Replicação**.
2. Na página Replicação, clique em **Par de servidores**.
3. Conclua as etapas no assistente Incluir par de servidores.

Sobre Esta Tarefa

Proteger um conjunto de armazenamentos de contêiner de diretório faz backup de extensões de dados para outro conjunto de armazenamentos e pode melhorar o desempenho para a replicação de nó. Quando a replicação de nó é iniciada, as extensões de dados que já foram submetidas a backup por meio da proteção do conjunto de armazenamentos são ignoradas, o que reduz o tempo de processamento de replicação. É possível planejar a proteção de conjuntos de armazenamentos várias vezes por dia para acompanhar mudanças nos dados.

Ao proteger um conjunto de armazenamentos, você não usa recursos que replicam dados e metadados existentes, o que melhora o desempenho do servidor. É necessário usar conjuntos de armazenamentos de contêiner de diretório se você desejar proteger e fazer backup apenas do conjunto de armazenamentos.

Estratégia de proteção alternativa: Como uma alternativa ao uso da replicação, é possível proteger dados em conjuntos de armazenamentos de contêiner de diretório copiando os dados para conjuntos de armazenamento de cópia do contêiner. Os dados em conjuntos de armazenamento de cópia do contêiner são armazenados em volumes de fita. Cópias de fita que são armazenadas externamente fornecem proteção de recuperação de desastre adicional em um ambiente replicado.

Procedimento

1. Como alternativa, para ativar a proteção do conjunto de armazenamentos, é possível usar o comando **PROTECT STGPOOL** do servidor de origem para fazer backup de extensões de dados em um conjunto de armazenamentos de contêiner de diretório. Por exemplo, para proteger um conjunto de armazenamentos de contêiner de diretório chamado POOL1, emita o seguinte comando:

   ```
   protect stgpool pool1
   ```

   Como parte da operação do comando **PROTECT STGPOOL**, as extensões corrompidas no conjunto de armazenamentos de destino são reparadas. Para serem reparadas, as extensões já devem ser marcadas como corrompidas no servidor de destino. Por exemplo, um comando **AUDIT CONTAINER** pode identificar o dano no conjunto de armazenamentos de destino antes de o comando **PROTECT STGPOOL** ser emitido.
2. Opcional: Se as extensões corrompidas foram reparadas no conjunto de armazenamentos de destino e você proteger vários conjuntos de armazenamentos de origem em um conjunto de armazenamentos de destino, conclua as etapas a seguir para garantir um reparo completo:
   a. Emita o comando **PROTECT STGPOOL** para todos os conjuntos de armazenamentos de origem para reparar quantos danos for possível.
   b. Emita o comando **PROTECT STGPOOL** novamente para todos os conjuntos de armazenamentos de origem. Para esta segunda operação, use o parâmetro **FORCERECONCILE=YES**. Esta etapa garante que todos os reparos de outros conjuntos de origem sejam reconhecidos adequadamente para todos os conjuntos de armazenamentos de origem.

Resultados

Se um conjunto de armazenamentos do contêiner de diretório estiver protegido, será possível reparar o conjunto de armazenamentos se ocorrer um dano, usando o comando **REPAIR STGPOOL**.

Restrição: Se você replicar nós clientes, mas não proteger o conjunto de armazenamentos de contêiner de diretório, não será possível reparar o conjunto de armazenamentos.

O que Fazer Depois

Conclua as seguintes ações:

1. Para visualizar o status da carga de trabalho de replicação, siga as instruções em Capítulo 13, “Lista de verificação de monitoramento diária”, na página 83.
2. Linux Se o servidor IBM Spectrum Protect replicar nós para um servidor remoto, determine se a tecnologia Aspera Fast Adaptive Secure Protocol (FASP) pode melhorar o rendimento de dados para o servidor remoto. Siga as instruções em Determinando se a tecnologia Aspera FASP pode otimizar a transferência de dados em seu ambiente de sistema.

Referências relacionadas:

Reparando e recuperando dados em conjuntos de armazenamentos de contêiner de diretório

AUDIT CONTAINER (Verificar a consistência de informações do banco de dados para um conjunto de armazenamentos de contêineres de diretório)

PROTECT STGPOOL (Proteger dados do conjunto de armazenamentos)

Informações relacionadas:

FAQs (Perguntas mais frequentes) sobre os conjuntos de armazenamentos de contêiner de diretório

FAQs (Perguntas mais frequentes) sobre os conjuntos de armazenamentos de contêiner em nuvem

Modificando configurações de replicação

Modifique configurações de replicação no Operations Center. Altere as configurações, como o número de sessões de replicação, regras de replicação e os dados que você deseja replicar, o planejamento de replicação e a carga de trabalho de replicação.

Sobre Esta Tarefa

Pode ser necessário customizar suas configurações de replicação nos seguintes cenários:

- Mudanças nas prioridades de dados
- Mudanças nas regras de replicação
- Requisito para que um servidor diferente seja o servidor de destino
- Processos planejados que afetam negativamente o desempenho do servidor

Procedimento

Use o Operations Center para modificar configurações de replicação.

Tarefa	Procedimento
Altere uma regra de replicação.	1. Na página Servidores, clique em **Detalhes**. 2. Na página Detalhes, clique em **Propriedades**. 3. Na seção **Replicação**, escolha a regra de replicação que deseja aplicar: **Regra de archive padrão**, **Regra de backup padrão** ou **Regra de gerenciamento de espaço padrão**. 4. Clique em **Salvar**.
Especifique a duração em que os registros de replicação ficam retidos.	1. Na página Servidores, clique em **Detalhes**. 2. Na página Detalhes, clique em **Propriedades**. 3. Na seção **Replicação**, insira o número de dias em que os registros de replicação devem ficar retidos no campo **Reter histórico de replicação**. Como alternativa, selecione a caixa de seleção **Não reter** se não precisar de registros de replicação. 4. Clique em **Salvar**.
Especifique um servidor de replicação de destino.	1. Na página Servidores, clique em **Detalhes**. 2. Na página Detalhes, clique em **Propriedades**. 3. Na seção **Replicação**, especifique o servidor de destino. 4. Clique em **Salvar**.
Cancele um processo de replicação.	1. Na página Servidores, clique em **Tarefas ativas**. 2. Selecione o processo ou sessão que você deseja cancelar. 3. Clique em **Cancelar**.

Configurando diferentes políticas de retenção para o servidor de origem e o servidor de destino

É possível configurar políticas no servidor de replicação de destino, que gerencia os dados replicados do nó cliente, de forma diferente do que no servidor de origem. Por exemplo, é possível manter várias versões de arquivos diferentes nos servidores de origem e de destino.

Procedimento

1. No servidor de replicação de origem, valide a configuração de replicação e verifique se o servidor de replicação de origem pode se comunicar com o servidor de replicação de destino, emitindo o comando **VALIDATE REPLICATION**. Por exemplo, valide a configuração usando o nome de um nó cliente que está sendo replicado:

   ```
   validate replication node1 verifyconnection=yes
   ```

2. No servidor de replicação de origem, emita o comando **VALIDATE REPLPOLICY** para revisar as diferenças entre as políticas nos servidores de origem e destino. Por exemplo, para exibir as diferenças entre as políticas no servidor de origem e no servidor de destino, CVT_SRV2, emita o comando a seguir a partir do servidor de origem:

   ```
   validate replpolicy cvt_srv2
   ```

3. Atualize as políticas no servidor de destino, se necessário.

   Dica: É possível usar o Operations Center para modificar as políticas no servidor de destino. Siga as instruções em "Editando políticas" na página 117. Por exemplo, para manter versões inativas dos arquivos durante menos tempo no servidor de destino do que no servidor de origem, reduza a configuração dos **Backups** nas classes de gerenciamento que se aplicam aos dados replicados do cliente.

4. Ative o servidor de replicação de destino para usar suas políticas para gerenciar os dados replicados do nó cliente, emitindo o comando **SET DISSIMILARPOLICIES** no servidor de origem. Por exemplo, para ativar as políticas no servidor de replicação de destino, CVT_SRV2, emita o comando a seguir no servidor de origem:

   ```
   set dissimilarpolicies cvt_srv2 on
   ```

   A próxima vez em que o processo de replicação for executado, as políticas no servidor de replicação de destino serão usadas para gerenciar os dados replicados do nó cliente.

   Dica: Se você configurar a replicação usando o Operations Center e as políticas nos servidores de replicação de origem e de destino não corresponderem, a política especificada para o servidor de replicação de origem será usada. Se você ativou as políticas no servidor de replicação de destino usando o comando **SET DISSIMILARPOLICIES**, a política especificada para o servidor de replicação de destino será usada. Se o servidor de replicação de destino não tiver a política que é usada pelo nó no servidor de replicação de origem, a política STANDARD será usada.

Referências relacionadas:

EXPORT POLICY (Exportar informações de política)

SET DISSIMILARPOLICIES (Ativar as políticas no servidor de replicação de destino para gerenciar dados replicados)

VALIDATE REPLICATION (Validar replicação para um nó cliente)

VALIDATE REPLPOLICY (Verificar as políticas no servidor de replicação de destino)

Capítulo 21. Protegendo o servidor

Proteja o servidor do IBM Spectrum Protect e dados controlando o acesso a servidores e nós clientes, criptografando dados e mantendo níveis de acesso e senhas seguros.

Conceitos de segurança

É possível proteger o IBM Spectrum Protect de riscos de segurança usando protocolos de comunicação, protegendo senhas e fornecendo diferentes níveis de acesso para administradores.

Segurança da Camada de Transporte

É possível usar o protocolo de Secure Sockets Layer (SSL) ou de Segurança da Camada de Transporte (TLS) para fornecer segurança da camada de transporte para uma conexão segura entre servidores, clientes e agentes de armazenamento. Se você enviar dados entre o servidor, o cliente e o agente de armazenamento, use SSL ou TLS para criptografar os dados.

Dica: Qualquer documentação do IBM Spectrum Protect que indique "SSL" ou "selecionar SSL" se aplica ao TLS.

O SSL é fornecido pelo Global Security Kit (GSKit) que está instalado com o servidor do IBM Spectrum Protect que é usado pelo servidor, cliente e agente de armazenamento.

Restrição: Não use os protocolos SSL ou TLS para comunicações com uma instância de banco de dados do IBM Db2 usada por qualquer servidor do IBM Spectrum Protect.

Cada servidor, cliente ou agente de armazenamento que ativa o SSL deve usar um certificado autoassinado confiável ou obter um certificado exclusivo que seja assinado por uma autoridade de certificação (CA). É possível usar seus próprios certificados ou comprar certificados de uma CA. O certificado deve ser instalado e incluído no banco de dados de chaves no servidor, cliente ou agente de armazenamento do IBM Spectrum Protect. O certificado é verificado pelo cliente ou servidor SSL que solicita ou inicia a comunicação de SSL. Alguns certificados de CA são pré-instalados nos bancos de dados de chaves, por padrão.

O SSL é configurado de forma independente no servidor, cliente e agente de armazenamento do IBM Spectrum Protect.

Níveis de Autoridade

Com cada servidor IBM Spectrum Protect, há diferentes níveis de autoridade administrativa disponíveis que determinam quais tarefas um administrador pode concluir.

Após o registro, um administrador deve receber autoridade, sendo designado a um ou mais níveis de autoridade administrativa. Um administrador com autoridade do sistema pode concluir qualquer tarefa com o servidor e designar níveis de

autoridade a outros administradores usando o comando **GRANT AUTHORITY**. Os administradores com autoridade de política, de armazenamento ou de operador podem concluir subconjuntos de tarefas.

Um administrador pode registrar outros IDs de administrador, conceder níveis de autoridade a eles, renomear IDs, remover IDs e bloquear e desbloqueá-los do servidor.

Um administrador pode controlar o acesso a nós clientes específicos para IDs do usuário raiz e IDs do usuário não raiz. Por padrão, um ID do usuário não raiz não pode fazer backup de dados no nó. Use o comando **UPDATE NODE** para alterar as configurações do nó para ativar o backup.

Senhas

Por padrão, o servidor usa automaticamente a autenticação de senha. Com a autenticação de senha, todos os usuários devem inserir uma senha quando acessarem o servidor.

Use o Lightweight Directory Access Protocol (LDAP) para aplicar requisitos mais rigorosos para senhas. Para obter informações adicionais, consulte Gerenciando senhas e procedimentos de logon (V7.1.1).

Tabela 19. Características de autenticação de senha

Característica	Informações adicionais
Distinção entre maiúsculas e minúsculas	Não distingue entre maiúsculas e minúsculas.
Expiração de senha padrão	90 dias. O período de expiração começa quando um ID de administrador ou nó cliente é registrado pela primeira vez no servidor. Se a senha não for mudada nesse período, ela deverá ser mudada na próxima vez que o usuário acessar o servidor.
Tentativas de senha inválida	É possível configurar um limite nas tentativas consecutivas de senha inválida para todos os nós clientes. Quando o limite for excedido, o servidor bloqueará o nó.
Padrão de comprimento de senha	8 caracteres. O administrador pode especificar um comprimento mínimo. Começando com a Versão 8.1.4, o comprimento mínimo padrão para senhas do servidor mudou de 0 para 8 caracteres.

Segurança da Sessão

Segurança de sessão é o nível de segurança que é usado para a comunicação entre os nós clientes, clientes administrativos e servidores do IBM Spectrum Protect e é configurada usando o parâmetro **SESSIONSECURITY**.

O parâmetro **SESSIONSECURITY** pode ser configurado com um dos seguintes valores:

- O valor `STRICT` aplica o nível mais alto de segurança para a comunicação entre servidores, nós e administradores do IBM Spectrum Protect.
- O valor `TRANSITIONAL` especifica que o protocolo de comunicação existente é usado ao atualizar o software IBM Spectrum Protect para a V8.1.2 ou mais recente. Esse é o padrão. Quando o valor é **`SESSIONSECURITY=TRANSITIONAL`**, configurações de segurança mais restritas são automaticamente aplicadas quanto mais altas as versões do protocolo TLS utilizado e quando o software é atualizado para a V8.1.2 ou posterior. Após um nó, administrador ou servidor atender aos requisitos para o valor `STRICT`, a segurança de sessão é atualizada automaticamente para o valor `STRICT` e a entidade não poderá mais se autenticar usando uma versão anterior do cliente ou protocolos TLS anteriores.

  Nota: Não é necessário atualizar clientes de archive de backup para a V8.1.2 ou posterior antes de fazer upgrade de servidores. Depois de fazer upgrade de um servidor para V8.1.2 ou posterior, nós e administradores que usam versões anteriores do software continuarão a se comunicar com o servidor usando o valor `TRANSITIONAL` até que a entidade atenda aos requisitos para o valor `STRICT` . Da mesma forma, é possível fazer upgrade de clientes de archive de backup para a V8.1.2 ou posterior antes de fazer upgrade de seus servidores do IBM Spectrum Protect, mas não é obrigatório atualizar os servidores primeiro. A comunicação entre servidores e clientes não será interrompida.

Para obter mais informações sobre os valores do parâmetro **`SESSIONSECURITY`**, consulte os comandos a seguir.

Tabela 20. Comandos utilizados para configurar o parâmetro SESSIONSECURITY

Entidade	Command
Nós clientes	• REGISTER NODE • UPDATE NODE
Administradores	• REGISTER ADMIN • UPDATE ADMIN
Servidores	• DEFINE SERVER • UPDATE SERVER

Os administradores que autenticam usando o comando **`DSMADMC`**, o comando **`DSMC`** ou o programa dsm não podem se autenticar usando uma versão anterior após executar a autenticação usando a V8.1.2 ou mais recente. Para resolver problemas de autenticação para administradores, consulte as seguintes dicas:

Dicas:

- Assegure-se de fazer upgrade de todos os softwares IBM Spectrum Protect que a conta do administrador usa para efetuar logon para a V8.1.2 ou mais recente. Se uma conta de administrador efetuar logon em vários sistemas, assegure-se de que o certificado do servidor esteja instalado em cada sistema.
- Depois que um administrador é autenticado no servidor com êxito usando as versões de software V8.1.2, V7.1.8 ou mais recentes, ele não pode mais se autenticar nesse servidor usando as versões de cliente ou de servidor anteriores a essas. Um comando do administrador pode ser emitido a partir de qualquer sistema.
- Se necessário, crie uma conta do administrador separada para usar somente com clientes e servidores que estão usando o software V8.1.1 ou anterior.

Force o nível mais alto de segurança para a comunicação com o servidor IBM Spectrum Protect, assegurando que todos os nós, administradores e servidores usem a segurança de sessão STRICT. É possível usar o comando **SELECT** para determinar quais servidores, nós e administradores estão usando a segurança de sessão `TRANSITIONAL` e devem ser atualizados para usar a segurança de sessão `STRICT`.

Tarefas relacionadas:

Protegendo Comunicações

Gerenciando administradores

Um administrador que tem autoridade do sistema pode concluir qualquer tarefa com o servidor IBM Spectrum Protect, incluindo designar níveis de autoridade a outros administradores. Para concluir algumas tarefas, deve-se ter recebido autoridade sendo designado a um ou mais níveis de autoridade.

Procedimento

Conclua as seguintes tarefas para modificar as configurações do administrador.

Tarefa	Procedimento

Incluir um administrador.	Para incluir um administrador, ADMIN1, com autoridade do sistema e especificar uma senha, conclua as etapas a seguir:
	1. Registre o administrador e especifique **Pa$#$twO** como a senha emitindo o seguinte comando:
	`register admin admin1 Pa$#$twO`
	2. Conceda autoridade do sistema ao administrador emitindo o seguinte comando:
	`grant authority admin1 classes=system`

Alterar autoridade administrativa.	Altere o nível de autoridade de um administrador, ADMIN1.
	• Conceda autoridade do sistema ao administrador emitindo o seguinte comando:
	`grant authority admin1 classes=system`
	• Revogue a autoridade do sistema para o administrador emitindo o seguinte comando:
	`revogue a autoridade admin1 classes=system`

Remover administradores.	Remova um administrador, ADMIN1, do acesso ao servidor do IBM Spectrum Protect emitindo o seguinte comando: `remove admin admin1`
Impedir temporariamente o acesso ao servidor.	Bloqueie ou desbloqueie um administrador usando o comando **LOCK ADMIN** ou **UNLOCK ADMIN**.

Alterando requisitos de senha

É possível mudar o limite mínimo de senha, comprimento de senha, expiração de senha e ativar ou desativar a autenticação para o IBM Spectrum Protect.

Sobre Esta Tarefa

Ao aplicar a autenticação de senha e gerenciar restrições de senha, você protege seus dados e seus servidores contra possíveis riscos de segurança.

Procedimento

Conclua as seguintes tarefas para alterar os requisitos de senha para servidores do IBM Spectrum Protect.

Tabela 21. Tarefas de autenticação para servidores do IBM Spectrum Protect

Tarefa	Procedimento
Configurar um limite para tentativas de senha inválida.	1. Na página Servidores no Operations Center, selecione o servidor. 2. Clique em **Detalhes**, e, em seguida, clique na guia **Propriedades**. 3. Configure o número de tentativas inválidas no campo **Limite de tentativas de conexão inválidas**. O valor padrão na instalação é 0.
Configure um comprimento mínimo para senhas.	1. Na página Servidores no Operations Center, selecione o servidor. 2. Clique em **Detalhes** e, em seguida, clique na guia **Propriedades**. 3. Configure o número de caracteres no campo **Comprimento mínimo de senha**.
Configure o período de expiração para senhas.	1. Na página Servidores no Operations Center, selecione o servidor. 2. Clique em **Detalhes** e, em seguida, clique na guia **Propriedades**. 3. Configure o número de dias no campo **Expiração comum de senha**.
Desativar autenticação de senha.	Por padrão, o servidor usa automaticamente a autenticação de senha. Com a autenticação de senha, todos os usuários devem inserir uma senha para acessar o servidor. É possível desativar a autenticação de senha somente para senhas que são autenticadas com o servidor (LOCAL). Desativando a autenticação de senha, aumenta-se o risco de segurança para o servidor.

Tabela 21. Tarefas de autenticação para servidores do IBM Spectrum Protect (continuação)

Tarefa	Procedimento

Configurar um método de autenticação padrão.	Emita o comando **SET DEFAULTAUTHENTICATION**. Por exemplo, para usar o servidor como o método de autenticação padrão, emita o comando a seguir:
	`set defaultauthentication local`
	
	Para atualizar um nó cliente para ser autenticado com o servidor, inclua `AUTHENTICATION=LOCAL` no comando **UPDATE NODE**:
	`update node authentication=local`

Conceitos relacionados:

- Autenticando usuários do IBM Spectrum Protect usando um servidor LDAP
- Gerenciando senhas e procedimentos de logon (V7.1.1)

Protegendo o IBM Spectrum Protect no sistema

Proteja o sistema em que o servidor do IBM Spectrum Protect é executado para evitar acesso não autorizado.

Procedimento

Certifique-se de que usuários não autorizados não possam acessar os diretórios do banco de dados do servidor e a instância do servidor. Mantenha as configurações de acesso para esses diretórios configurados durante a implementação.

Restringindo o acesso de usuário ao servidor

Os níveis de autoridade determinam o que um administrador pode fazer com o servidor do IBM Spectrum Protect. Um administrador com autoridade do sistema pode concluir qualquer tarefa com o servidor. Os administradores com autoridade de política, de armazenamento ou de operador podem concluir subconjuntos de tarefas.

Procedimento

1. Depois de registrar um administrador usando o comando **REGISTER ADMIN**, use o comando **GRANT AUTHORITY** para configurar o nível de autoridade do administrador. Para obter detalhes sobre como configurar e mudar a autoridade, consulte "Gerenciando administradores" na página 152.
2. Para controlar a autoridade de um administrador para concluir algumas tarefas, use as duas seguintes opções do servidor:
   a. É possível selecionar o nível de autoridade que um administrador deve ter para emitir comandos **QUERY** e **SELECT** com a opção do servidor **QUERYAUTH**. Por padrão, o nível de autoridade é obrigatório. É possível alterar o requisito para um dos níveis de autoridade, incluindo o sistema.
   b. É possível especificar que a autoridade do sistema é obrigatória para comandos que fazem o servidor gravar em um arquivo externo com a opção do servidor **REQSYSAUTHOUTFILE**. Por padrão, autoridade do sistema é obrigatória para esses comandos.

3. É possível restringir o backup de dados em um nó de cliente somente a IDs do usuário raiz ou usuários autorizados. Por exemplo, para limitar backups ao ID do usuário raiz, emita o comando **REGISTER NODE** ou **UPDATE NODE** e especifique o parâmetro **BACKUPINITIATION=root**:

   ```
   update node backupinitiation=root
   ```

Limitando o acesso por meio de restrições de porta

Limite o acesso ao servidor aplicando restrições de porta.

Sobre Esta Tarefa

Pode ser necessário restringir o acesso a servidores específicos, com base em seus requisitos de segurança. O servidor IBM Spectrum Protect pode ser configurado para atender em quatro portas TCP/IP: duas que podem ser usadas para protocolos TCP/IP regulares ou protocolos Secure Sockets Layer (SSL)/Segurança da Camada de Transporte (TLS) e duas que podem ser usadas somente para o protocolo SSL/TLS.

Procedimento

É possível configurar as opções do servidor para especificar a porta requerida, conforme listado em Tabela 22.

Tabela 22. Opções do servidor e acesso à porta

Opção do servidor	Acesso à porta
TCPPORT	Especifica o número da porta na qual o driver de comunicação TCP/IP do servidor deve aguardar solicitações de sessões do cliente. Esta porta atende sessões ativadas para TCP/IP e SSL. O valor padrão é 1500.
TCPADMINPORT	Especifica o número da porta na qual o driver de comunicação TCP/IP do servidor deve aguardar solicitações de sessões diferentes das sessões do cliente. Esta porta atende sessões ativadas para TCP/IP e SSL. O padrão é o valor **TCPPORT**. Use essa opção para separar o tráfego do cliente administrador do tráfego do cliente regular que usa as opções **TCPPORT** e **SSLTCPPORT**.
SSLTCPPORT	Especifica o endereço de porta TCP/IP SSL para um servidor. Esta porta atende somente sessões ativadas para SSL. Um valor de porta padrão não está disponível.
SSLTCPADMINPORT	Especifica o endereço de porta no qual o driver de comunicação TCP/IP do servidor aguarda solicitações de sessões ativadas para SSL. Um valor de porta padrão não está disponível. Use essa opção para separar o tráfego do cliente administrador do tráfego do cliente regular que usa as opções **TCPPORT** e **SSLTCPPORT**.

Restrições:

As seguintes restrições se aplicam ao especificar as portas de servidor somente SSL (**SSLTCPPORT** e **SSLTCPADMINPORT**):

- Ao especificar a porta somente SSL do servidor para **LLADDRESS** no comando **DEFINE SERVER** ou **UPDATE SERVER**, é preciso especificar também o parâmetro **SSL=YES**.

- Ao especificar a porta somente SSL do servidor para a opção **TCPPORT** do cliente, é preciso também especificar **YES** para a opção do cliente SSL.

Referências relacionadas:

"Planejando acesso ao firewall" na página 31

Capítulo 22. Parando e iniciando o servidor

Antes de concluir tarefas de manutenção ou reconfiguração, pare o servidor. Em seguida, inicie o servidor no modo de manutenção. Quando concluir as tarefas de manutenção ou reconfiguração, reinicie o servidor no modo de produção.

Antes de Iniciar

Deve-se ter privilégio de sistema ou operador para parar e iniciar o servidor IBM Spectrum Protect.

Parando o Servidor

Antes de parar o servidor, prepare o sistema assegurando que todas as operações de backup de banco de dados sejam concluídas e que todos os outros processos e sessões estejam terminados. Dessa forma, é possível encerrar o servidor com segurança e assegurar que os dados sejam protegidos.

Sobre Esta Tarefa

Ao emitir o comando **HALT** para parar o servidor, ocorrem as seguintes ações:

- Todos os processos e sessões do nó cliente são cancelados.
- Todas as transações atuais são interrompidas. (As transações serão recuperadas quando o servidor for reiniciado.)

Procedimento

Para preparar o sistema e parar o servidor, conclua as etapas a seguir:

1. Evite que novas sessões do nó cliente sejam iniciadas emitindo o comando **DISABLE SESSIONS**:

   ```
   disable sessions all
   ```

2. Determine se os processos ou sessões do nó cliente estão em andamento concluindo as etapas a seguir:
   a. Na página Visão geral do Operations Center, visualize a área Atividade para o número total de processos e sessões que estão atualmente ativos. Se os números diferirem significativamente dos números comuns que são exibidos durante a rotina diária de gerenciamento de armazenamento, visualize outros indicadores de status no Operations Center para verificar se há um problema.
   b. Visualize o gráfico na área Atividade para comparar a quantia de tráfego de rede nos períodos a seguir:
      - O período atual, ou seja, o período mais recente de 24 horas
      - O período anterior, ou seja, as 24 horas antes do período atual

      Se o gráfico para o período anterior representar a quantia esperada de tráfego, as diferenças significativas no gráfico para o período atual poderão indicar um problema.
   c. Na página Servidores, selecione um servidor cujos processos e sessões você deseja visualizar e clique em **Detalhes**. Se o servidor não estiver registrado como um servidor do hub ou spoke no Operations Center, obtenha informações sobre processos usando comandos administrativos. Emita o

comando **QUERY PROCESS** para os processos de consulta e obtenha informações sobre as sessões emitindo o comando **QUERY SESSION**.

3. Aguarde até que as sessões do nó cliente sejam concluídas ou cancele-as. Para cancelar processos e sessões, conclua as etapas a seguir:
   - Na página Servidores, selecione um servidor cujos processos e sessões você deseja visualizar e clique em **Detalhes**.
   - Clique na guia Tarefas ativas e selecione um ou mais processos, sessões ou uma combinação de ambos que você deseja cancelar.
   - Clique em **Cancelar**.
   - Se o servidor não estiver registrado como um servidor do hub ou spoke no Operations Center, cancele as sessões usando comandos administrativos. Emita o comando **CANCEL SESSION** para cancelar uma sessão e cancele processos usando o comando **CANCEL PROCESS**.

     Dica: Se o processo que você deseja cancelar estiver aguardando a montagem de um volume da fita, a solicitação de montagem será cancelada. Por exemplo, se você emitir um comando **EXPORT**, **IMPORT** ou **MOVE DATA**, o comando poderá iniciar um processo que requer a montagem de um volume da fita. No entanto, se um volume da fita estiver sendo montado por uma biblioteca automatizada, a operação de cancelamento não poderá entrar em vigor até que o processo de montagem esteja concluído. Dependendo de seu ambiente do sistema, isso pode levar alguns minutos.
4. Pare o servidor emitindo o comando **HALT**:

   ```
   halt
   ```

Iniciando o servidor para tarefas de manutenção ou reconfiguração

Antes de iniciar as tarefas de manutenção ou reconfiguração do servidor, inicie o servidor no modo de manutenção. Ao iniciar o servidor no modo de manutenção, desative as operações que possam interromper suas tarefas de manutenção ou de reconfiguração.

Sobre Esta Tarefa

Inicie o servidor no modo de manutenção, executando o utilitário **DSMSERV** com o parâmetro **MAINTENANCE**.

As operações a seguir são desativadas no modo de manutenção:

- Planejamentos de comandos administrativos
- Planejamentos de Clientes
- Reclamação do espaço de armazenamento no servidor
- Expiração de inventário
- Migração dos conjuntos de armazenamentos

Além disso, os clientes são impedidos de iniciar as sessões com o servidor.

Dicas:

- Não é necessário editar o arquivo de opções do servidor, `dsmserv.opt`, para iniciar o servidor no modo de manutenção.
- Enquanto o servidor estiver em execução no modo de manutenção, é possível iniciar manualmente a recuperação de espaço de armazenamento, expiração de inventário e processos de migração do conjunto de armazenamentos.

Procedimento

Para iniciar o servidor no modo de manutenção, emita o comando a seguir:

```
dsmserv maintenance
```

Dica: Para visualizar um vídeo sobre como iniciar o servidor no modo de manutenção, veja Iniciando um servidor no modo de manutenção.

O que Fazer Depois

Para continuar as operações do servidor, conclua as etapas a seguir:

1. Encerre o servidor, emitindo o comando **HALT**:

   ```
   halt
   ```

2. Inicie o servidor, usando o método que você usa no modo de produção. Siga as instruções para o seu sistema operacional:
   - AIX Iniciando a Instância do Servidor
   - Linux Iniciando a Instância do Servidor
   - Windows Iniciando a Instância do Servidor

As operações que foram desativadas durante o modo de manutenção foram reativadas.

Capítulo 23. Planejando fazer upgrade do servidor

Quando um fix pack ou correção temporária é disponibilizado, é possível fazer upgrade do servidor IBM Spectrum Protect para aproveitar as melhorias do produto. É possível fazer upgrade de servidores e clientes em momentos diferentes. Certifique-se de concluir as etapas de planejamento antes de fazer upgrade do servidor.

Sobre Esta Tarefa

Siga estas diretrizes:

- O método preferencial é fazer upgrade do servidor usando o assistente de instalação. Depois de iniciar o assistente, na janela IBM Installation Manager, clique no ícone **Atualizar**; não clique no ícone **Instalar** ou **Modificar**.
- Se os upgrades estiverem disponíveis para o componente do servidor e o componente Operations Center, selecione as caixas de seleção para fazer upgrade dos dois componentes.

Procedimento

1. Revise a lista de fix packs e de correções temporárias. Consulte nota técnica 1239415.
2. Revise as melhorias de produto, que são descritas em arquivos leia-me.

   Dica: Quando obtiver o arquivo de pacote de instalação do Site de Suporte do IBM Spectrum Protect, também será possível acessar o arquivo leia-me.
3. Certifique-se de que a versão para a qual você atualizou seu servidor seja compatível com outros componentes, como agentes de armazenamento e clientes de biblioteca. Consulte nota técnica 1302789.
4. Se sua solução incluir servidores ou clientes em um nível anterior à V7.1, revise as diretrizes para assegurar que as operações de backup e archive do cliente não sejam interrompidas. Consulte nota técnica 1053218.
5. Revise as instruções de upgrade. Certifique-se de fazer backup do banco de dados do servidor, das informações de configuração do dispositivo e do arquivo do histórico de volume.

O que Fazer Depois

Para instalar um fix pack ou correção temporária, siga as instruções para seu sistema operacional:

- AIX Instalando um Fix Pack do Servidor IBM Spectrum Protect
- Linux Instalando um Fix Pack do Servidor IBM Spectrum Protect
- Windows Instalando um Fix Pack do Servidor IBM Spectrum Protect

Informações relacionadas:

Processo de upgrade e migração - Perguntas mais frequentes

Capítulo 24. Preparando-se para uma indisponibilidade ou atualização do sistema

Prepare o IBM Spectrum Protect para manter seu sistema em um estado consistente durante uma indisponibilidade de energia ou atualização do sistema planejada.

Sobre Esta Tarefa

Certifique-se de planejar atividades regularmente para gerenciar, proteger e manter o servidor.

Procedimento

1. Cancele processos e sessões que estão em andamento concluindo as etapas a seguir:
   a. No Operations Center, na página Servidores, selecione um servidor para o qual deseja visualizar processos e sessões e clique em **Detalhes**.
   b. Clique na guia **Tarefas ativas** e selecione um ou mais processos, sessões ou uma combinação de ambos que você deseja cancelar.
   c. Clique em **Cancelar**.
2. Pare o servidor emitindo o comando **HALT**:

   ```
   halt
   ```

   Dica: É possível emitir o comando de parada do Operations Center passando o mouse sobre o ícone **Configurações** e clicando em **Construtor de comando**. Em seguida, selecione o servidor, digite `halt` e pressione **Enter**.

Capítulo 25. Implementando um plano de recuperação de desastres

Implemente uma estratégia de recuperação de desastre para recuperar seus aplicativos se ocorrer um desastre e para assegurar alta disponibilidade do servidor.

Sobre Esta Tarefa

Determine os seus requisitos de recuperação de desastre identificando as prioridades de negócio para recuperação do nó cliente, os sistemas que você usa para recuperar dados e se os nós cliente têm conectividade para um servidor de recuperação. Use replicação e proteção do conjunto de armazenamentos para proteger dados. Também é necessário determinar a frequência com que os conjuntos de armazenamentos de contêiner de diretório são protegidos.

Concluindo drills de recuperação

Planeje drills de recuperação de desastre para preparar-se para auditorias que certificam a recuperabilidade do servidor IBM Spectrum Protect e para assegurar que os dados possam ser restaurados e as operações continuadas após uma indisponibilidade. Um drill também ajuda a assegurar que todos os dados possam ser restaurados e as operações continuadas antes de ocorrer uma situação crítica.

Sobre Esta Tarefa

Com uma solução de disco multisite, use a replicação de nó para assegurar que os dados estejam disponíveis em um servidor de destino no site de recuperação e o tempo de recuperação seja rápido. Quando houver uma indisponibilidade, o servidor de origem pode executar failover automaticamente para um servidor de destino para recuperação de dados. Se ocorrer um desastre e o servidor de origem estiver indisponível, os nós clientes podem automaticamente registrar informações sobre o servidor de replicação de destino no arquivo de opções do cliente. Pode ser necessário atualizar manualmente o arquivo de opções do cliente para clientes mais antigos.

Procedimento

1. Restaure manualmente os dados de um servidor de replicação de destino, atualize o arquivo de opções do cliente para apontar para o servidor de replicação de destino. Mudanças nas configurações de replicação de nó não são necessárias.
2. Configure um nó cliente para armazenar dados em um servidor de replicação de destino.

   Restrição: Os nós clientes que normalmente fazem backup de dados para um servidor de replicação de origem não podem fazer backup de dados para os nós clientes que são replicados no servidor de replicação de destino.
3. Teste a recuperação de dados de cliente concluindo as etapas a seguir:
   a. Restaure o sistema do cliente para um sistema operacional semelhante. Use os mesmos nomes do sistema de arquivos com a mesma quantidade de espaço no arquivo no sistema de arquivos

b. Em um sistema que possui espaço suficiente para os dados, restaure os dados.
c. Verifique se o cliente foi restaurado com sucesso. Por exemplo, se você restaurar uma máquina virtual, verifique se a máquina virtual está ligada e verifique se os arquivos estão disponíveis.

Tarefas relacionadas:

Replicando dados do nó cliente após uma restauração de banco de dados (V7.1.1)

Capítulo 20, “Gerenciando a replicação”, na página 143

Capítulo 26. Recuperando-se de perda de dados ou de indisponibilidades do sistema

É possível usar o IBM Spectrum Protect para recuperar dados que foram perdidos quando ocorreu um desastre ou uma indisponibilidade do sistema. É possível recuperar conjuntos de armazenamentos de contêiner de diretório, dados de cliente e bancos de dados.

Antes de Iniciar

Planeje as cargas de trabalho do cliente e do servidor para atingir o melhor desempenho para o seu ambiente de armazenamento. Emita os comandos **PROTECT STGPOOL** e **REPLICATE NODE** como parte do planejamento. Proteja o conjunto de armazenamentos antes de replicar o nó cliente. Quando a replicação de nó for iniciada, as extensões de dados que já são replicadas por meio da proteção do conjunto de armazenamentos serão ignoradas, o que reduz o tempo de processamento de replicação.

Procedimento

Use os seguintes métodos de recuperação com base no componente que você deve recuperar.

Componente a ser recuperado	Procedimento	Informações adicionais
Conjunto de armazenamentos de contêiner de diretório	Para recuperar conjuntos de armazenamentos de contêiner de diretório, conclua as etapas a seguir: 1. Varra extensões de dados danificadas no conjunto de armazenamentos de contêiner de diretório usando o comando **AUDIT CONTAINER** e especificando o parâmetro **ACTION=SCANALL**. 2. Repare extensões de dados danificadas no conjunto de armazenamentos de contêiner de diretório usando o comando **REPAIR STGPOOL**. **Restrição:** Só é possível reparar um conjunto de armazenamentos se o conjunto de armazenamentos estiver protegido. 3. Remova extensões de dados danificadas usando o comando **AUDIT CONTAINER** e especificando o parâmetro **ACTION=REMOVEDAMAGED**.	"Reparando conjuntos de armazenamentos" na página 172

Componente a ser recuperado	Procedimento	Informações adicionais
Dados de cliente	**Pré-requisitos:** • O servidor de replicação de origem, o servidor de replicação de destino e o cliente devem estar no nível da V7.1 ou mais recente. Se algum dos servidores estiver em um nível anterior, o failover automático será desativado e você deve contar com o failover manual. Configure manualmente o cliente para executar failover automaticamente no servidor de destino para recuperação de dados. Se você ativou o cliente para failover do cliente automatizado, será possível recuperar os dados usando a função de failover automático. É possível verificar se a opção `usereplicationfailover` não está no arquivo de opções do cliente ou se está configurada como `yes`. Recupere dados do servidor de destino quando o servidor de origem estiver indisponível devido a uma indisponibilidade usando o failover automático. **Dica:** • Use o comando **SET FAILOVERHLADDRESS** para especificar o endereço IP para o servidor de replicação durante o failover, se o endereço for diferente do endereço IP especificado para o processo de replicação.	• "Recuperando dados danificados de uma cópia replicada" na página 171 • SET FAILOVERHLADDRESS (Configurar um endereço de alto nível de failover)
Banco de Dados	**Pré-requisitos:** • Para restaurar o banco de dados após um desastre, é necessário ter uma cópia do arquivo de configuração de dispositivo atual. O arquivo de configuração de dispositivo não pode ser recriado. • Certifique-se de que tenha uma versão de backup do banco de dados. Restaure o banco de dados do IBM Spectrum Protect para o estado mais atual ou para um momento específico usando o utilitário do servidor **DSMSERV RESTORE DB**.	DSMSERV RESTORE DB (Restaurar o banco de dados)

Referências relacionadas:

AUDIT CONTAINER (Verificar a consistência de informações do banco de dados para um conjunto de armazenamentos de contêineres de diretório)

DSMSERV RESTORE DB (Restaurar o banco de dados)

Restaurando o banco de dados

Você pode ter que restaurar o banco de dados do IBM Spectrum Protect após um desastre. É possível restaurar o banco de dados para o estado mais atual ou para um momento específico. Deve-se ter volumes de backup de banco de dados completos, incrementais ou de captura instantânea para restaurar o banco de dados.

Antes de Iniciar

Se os diretórios de log do banco de dados e de recuperação forem perdidos, recrie-os antes de emitir o utilitário do servidor **DSMSERV RESTORE DB**. Por exemplo, use os seguintes comandos: AIX Linux

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

Windows

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

Restrições:

- Para restaurar o banco de dados para sua versão mais recente, deve-se localizar o diretório de log de archive. Se não for possível localizar o diretório, será possível restaurar o banco de dados apenas para um momento.
- Não é possível usar o Secure Sockets Layer (SSL) para operações de restauração do banco de dados.
- Se o nível da liberação do backup de banco de dados for diferente do nível da liberação do servidor que está sendo restaurado, não será possível restaurar o banco de dados do servidor. Por exemplo, se você estiver usando um servidor Versão 8.1 e tentar restaurar um banco de dados Versão 7.1, ocorrerá um erro.

Sobre Esta Tarefa

As operações de restauração do momento geralmente são usadas para situações, como recuperação de desastre ou para remover os efeitos de erros que podem causar inconsistências no banco de dados. Para recuperar o banco de dados para o momento em que ele foi perdido, recupere o banco de dados para sua versão mais recente.

Procedimento

Use o utilitário do servidor **DSMSERV RESTORE DB** para restaurar o banco de dados. Dependendo da versão do banco de dados que você deseja restaurar, escolha um dos métodos a seguir:

- Restaurar um banco de dados para sua versão mais recente. Por exemplo, use o seguinte comando:

  ```
  dsmserv restore db
  ```

- Restaurar um banco de dados para um momento. Por exemplo, para restaurar o banco de dados para uma série de backup que foi criada em 19 de abril de 2015, use o seguinte comando:

  ```
  dsmserv restore db todate=04/19/2015
  ```

O que Fazer Depois

Se você restaurou o banco de dados e existirem conjuntos de armazenamentos de contêiner de diretório no servidor, será necessário identificar inconsistências entre o banco de dados e o sistema de arquivos.

1. Se você restaurou o banco de dados para um momento e não atrasou a reutilização do conjunto de armazenamentos de contêiner de diretório, será necessário auditar todos os contêineres. Para auditar todos os contêineres, emita o seguinte comando:

   ```
   audit container stgpool
   ```

2. Se o servidor não puder identificar contêineres no sistema, conclua as etapas a seguir para exibir uma lista de contêineres:
   a. A partir de um cliente administrativo, emita o comando a seguir:

      ```
      select container_name from containers
      ```

   b. Do sistema de arquivos, emita o comando a seguir para o diretório do conjunto de armazenamentos no servidor de origem:

      Dica: O diretório do conjunto de armazenamentos é exibido na saída de comando:

      AIX Linux

      ```
      [ root@source ] $ls -lR
      ```

      Windows

      ```
      > c: \source_stgpooldir dir /s
      ```

   c. Compare os contêineres que estão listados no sistema de arquivos e o servidor.
   d. Emita o comando **AUDIT CONTAINER** e especifique o contêiner que está ausente da saída do servidor. Especifique o parâmetro **ACTION=REMOVEDAMAGED** para excluir o contêiner.
   e. Para assegurar que os contêineres sejam excluídos no sistema de arquivos, revise as mensagens que são exibidas.

      Dica: Após uma operação de restauração do banco de dados, se existirem contêineres no sistema de arquivos que não estão referenciados no banco de dados do servidor, o comando **QUERY STGPOOL** exibirá incorretamente o uso do conjunto de armazenamento. Ao restaurar um banco de dados para um momento, os contêineres podem permanecer no sistema de arquivos, mas não serão referenciados no banco de dados do servidor. Para ajudar a garantir estatísticas precisas sobre o uso do conjunto de armazenamento,

deve-se excluir manualmente quaisquer contêineres disponíveis no sistema de arquivos, mas não referenciados no banco de dados do servidor.

Tarefas relacionadas:

Replicando dados do nó cliente após uma restauração de banco de dados (V7.1.1)

Referências relacionadas:

AUDIT CONTAINER (Verificar a consistência de informações do banco de dados para um conjunto de armazenamentos de contêineres de diretório)

DSMSERV RESTORE DB (Restaurar o banco de dados)

Recuperando dados danificados de uma cópia replicada

Se um servidor de replicação de origem estiver indisponível, é possível recuperar dados danificados de uma cópia replicada que está armazenada no servidor de replicação de destino.

Antes de Iniciar

O nome do servidor especificado com o comando **SET REPLSERVER** deve corresponder ao nome de uma definição do servidor existente. Ele também deve ser o nome do servidor a ser usado como o servidor de replicação de destino. Se o nome do servidor especificado por esse comando não corresponder ao nome do servidor da definição de um servidor existente, o comando irá falhar.

Dica:

- Tome cuidado ao alterar ou remover um servidor de replicação de destino. Se você mudar um servidor de replicação de destino, os dados replicados do nó cliente serão enviados a um servidor de replicação de destino diferente. Se você remover um servidor de replicação de destino, os dados do nó de cliente não serão replicados.

Procedimento

1. Verifique o status de replicação dos dados no servidor de destino. O status de replicação indica se o backup mais recente foi replicado no servidor secundário.
2. Restaure dados de um servidor de replicação de destino configurando o servidor de replicação de origem como o servidor de replicação de destino. Por exemplo, se desejar configurar o servidor de replicação de origem como o servidor de replicação de destino, server1, emita o seguinte comando:

   ```
   set replserver server1
   ```

O que Fazer Depois

Ao restaurar o banco de dados do IBM Spectrum Protect em um servidor de replicação de origem, a replicação é desativada automaticamente. Antes de reativar a replicação, determine se as cópias de dados que estão no servidor de replicação de destino são necessárias.

Tarefas relacionadas:

Replicando dados do nó cliente após uma restauração de banco de dados (V7.1.1)

Reparando conjuntos de armazenamentos

Se ocorreu um desastre ou uma indisponibilidade do sistema, será possível reparar extensões de dados deduplicados em um conjunto de armazenamentos de contêiner de diretório.

Antes de Iniciar

Identifique inconsistências entre o banco de dados e o conjunto de armazenamentos de contêiner de diretório usando o comando **AUDIT CONTAINER**. Ao identificar extensões de dados danificadas no conjunto de armazenamentos de contêiner de diretório, é possível determinar quais extensões de dados reparar.

Antes de reparar um conjunto de armazenamentos, certifique-se de que o conjunto de armazenamentos esteja protegido, utilizando o comando **PROTECT STGPOOL**.

Procedimento

1. Para reparar um conjunto de armazenamentos de contêiner de diretório, use o comando **REPAIR STGPOOL**. Por exemplo, para reparar um conjunto de armazenamentos, STGPOOL1, emita o seguinte comando:

   ```
   repair stgpool stgpool1
   ```

2. Se o conjunto de armazenamentos danificado for especificado como um conjunto de armazenamentos de destino no comando **PROTECT STGPOOL** para um ou mais conjuntos de armazenamentos de origem, emita o comando **PROTECT STGPOOL** para todos os conjuntos de armazenamentos de origem.
3. Para assegurar que todos os dados danificados sejam identificados e reparados a partir de outros conjuntos de armazenamentos de origem, emita o comando **PROTECT STGPOOL** novamente a partir de todos os conjuntos de armazenamentos de origem e especifique o parâmetro **FORCERECONCILE=YES**.
4. Para remover objetos que fazem referência a dados danificados, emita o comando **AUDIT CONTAINER** e especifique o parâmetro **ACTION=REMOVEDAMAGED**.
5. Se o conjunto de armazenamentos danificado for um conjunto de armazenamentos de destino para a replicação de nó a partir de um ou mais servidores de origem, emita o comando **REPLICATE NODE** novamente a partir de todos os servidores de origem.
6. Quando o dano for reparado, emita o comando **PROTECT STGPOOL** para assegurar que o conjunto de armazenamentos seja protegido para outro conjunto de armazenamentos de contêiner de diretório.

O que Fazer Depois

Certifique-se de que nenhuma extensão de dados danificada seja exibida na saída usando o comando **QUERY DAMAGED**.

Referências relacionadas:

Reparando e recuperando dados em conjuntos de armazenamentos de contêiner de diretório

AUDIT CONTAINER (Verificar a consistência de informações do banco de dados para um conjunto de armazenamentos de contêineres de diretório)

QUERY DAMAGED (Consultar dados danificados em um conjunto de armazenamentos de contêiner em nuvem ou de contêiner-diretório)

REPAIR STGPOOL (Reparar um conjunto de armazenamentos de contêiner-diretório)

Parte 5. Apêndices

Apêndice. Recursos de Acessibilidade para a Família de Produtos IBM Spectrum Protect

Os recursos de acessibilidade ajudam os usuários que possuem uma deficiência, como mobilidade restrita ou visão limitada, a usar o conteúdo de tecnologia da informação com êxito.

Visão Geral

A família de produtos IBM Spectrum Protect inclui os principais recursos de acessibilidade a seguir:

- Operação apenas do teclado
- Operações que usam um leitor de tela

A família de produtos IBM Spectrum Protect usa o padrão W3C mais recente, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), para assegurar conformidade com o US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) e Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Para aproveitar os recursos de acessibilidade, use a liberação mais recente do seu leitor de tela e o último navegador da web que seja suportado pelo produto.

A documentação do produto no IBM Knowledge Center é ativada para acessibilidade. Os recursos de acessibilidade do IBM Knowledge Center estão descritos na seção de Acessibilidade da ajuda do IBM Knowledge Center (www.ibm.com/support/knowledgecenter/about/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).

Aviso

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. Este material pode estar disponível na IBM em outros idiomas. No entanto, pode ser necessário possuir uma cópia do produto ou da versão de produto no mesmo idioma para acessá-lo.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a um produto, programa ou serviço IBM não afirma ou significa que apenas que o 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 utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não concede ao Cliente nenhum direito sobre tais patentes. Pedidos de licenças devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO-INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Esta publicação pode conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode fazer aperfeiçoamentos e/ou alterações nos produtos ou programas descritos nesta publicação a qualquer momento sem aviso prévio.

As referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais contidos nesses websites não fazem parte dos materiais desse produto IBM e a utilização desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer outro contrato equivalente entre as partes.

Os dados de desempenho discutidos aqui são apresentados como derivados sob as condições de operação específicas. Os resultados reais podem variar.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas aos fornecedores desses produtos.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos incluem nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com os nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem

garantia de qualquer tipo. A IBM não poderá ser responsabilizada por quaisquer danos decorrentes ao uso dos programas de amostra.

Qualquer cópia, parte desses programas de amostra ou trabalho derivado deve incluir um aviso de copyright da seguinte forma: © (o nome de sua empresa) (ano). Partes deste código são derivadas dos Programas de Amostra da IBM Corp. © Copyright IBM Corp. _insira o ano ou anos_.

Marcas

IBM, o logotipo IBM e ibm.com são marcas registradas ou comerciais da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas comerciais IBM está disponível na web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Adobe é uma marca registrada da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Linear Tape-Open, LTO e Ultrium são marcas comerciais da HP, IBM Corp. e Quantum nos Estados Unidos e em outros países.

Intel e Itanium são marcas comerciais ou marcas registradas da Intel Corporation ou de suas subsidiárias nos Estados Unidos e em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows e Windows NT são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Java™ e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou de suas afiliadas.

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 de VMware, Inc. ou suas subsidiárias nos Estados Unidos e/ou em outros países.

Termos e Condições para a Documentação do Produto

As permissões para uso dessas publicações são concedidas sujeitas aos termos e condições a seguir.

Aplicabilidade

Esses termos e condições são adicionais a quaisquer termos de uso para o website da IBM.

utilizar o Personal

Você pode reproduzir estas publicações para seu uso pessoal não comercial desde que todos os avisos do proprietário sejam preservados. O Cliente não pode distribuir, exibir ou fazer trabalho derivado destas publicações, ou de parte delas, sem o consentimento expresso da IBM.

Uso comercial

É possível reproduzir, distribuir e exibir estas publicações exclusivamente dentro de sua empresa desde que todos os avisos do proprietário sejam preservados. O Cliente não pode fazer trabalhos derivados destas publicações ou reproduzir, distribuir ou exibir estas publicações, ou qualquer parte delas, fora de sua empresa, sem o consentimento expresso da IBM.

Direitos

Exceto como expressamente concedido nesta permissão, nenhuma outra permissão, licença ou direito é concedido, seja expresso ou implícito, para as publicações ou para quaisquer informações, dados, software ou outra propriedade intelectual nelas contidos.

A IBM reserva-se o direito de retirar as permissões concedidas aqui sempre que, a seu critério, o uso das publicações prejudicar seus interesses ou, conforme determinação da IBM, as instruções anteriores não estão sendo seguidas adequadamente.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto em conformidade total com todas as leis e regulamentos aplicáveis, incluindo todas as leis e regulamentos de exportação dos Estados Unidos.

A IBM NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

Considerações sobre política de privacidade

Os produtos de Software IBM, incluindo as soluções de software como serviço (“Ofertas de Software”), podem usar cookies ou outras tecnologias para coletar informações sobre o uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem permitir a coleta de informações identificáveis pessoalmente. Se esta Oferta de Software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies desta oferta serão apresentadas abaixo.

Esta Oferta de Software não usa cookies ou outras tecnologias para coletar informações pessoalmente identificáveis.

Se as configurações implementadas para esta Oferta de software fornecerem a você, como cliente, a capacidade de coletar informações de identificação pessoal de usuários finais por meio de cookies e outras tecnologias, é necessário buscar seu próprio conselho jurídico legal sobre quaisquer leis aplicáveis a este tipo de coleção de dados, incluindo quaisquer requisitos de aviso e consentimento.

Para obter informações adicionais sobre o uso de várias tecnologias, incluindo cookies, para estes propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy e a Declaração de privacidade on-line da IBM em http://www.ibm.com/privacy/details na seção intitulada “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service

Privacy Statement" em http://www.ibm.com/software/info/product-privacy.

Glossário

Está disponível um glossário com termos e definições para a família de produtos IBM Spectrum Protect.

Consulte o IBM Spectrum Protectglossário.

Índice Remissivo

A

aceitante do cliente
  configurando 123
  parando 128
  reiniciando 128
acesso
  limitar 155
  opções do servidor 155
arquivos RPM
  instalação para assistente gráfico 54
Aspera FASP 143, 144
Aspera Fast Adaptive Secure Protocol
  Veja Aspera FASP
assistente de configuração inicial
  configurar o 109
assistente gráfico
  arquivos RPM obrigatórios 54
atividades planejadas
  ajustando 141
atualização do sistema
  preparar 163
AUDIT CONTAINER 137
auditar conjunto de armazenamentos 137

C

capacidade de inventário 138
capacidade do banco de dados 138
capacidade do log ativo 138
capacidade do log de archive 138
classe de privilégio
  privilégio no sistema 152
clientes
  atualizando 131
  conectando ao servidor 120
  configurando 69, 121
  configurando para executar operações planejadas 123
  definir planejamentos 68
  desatribuir 142
  designar a planejamentos 69
  gerenciando operações 126
  incluindo 113
  instalação 69, 121
  mover 142
  protegendo 113
  registrando 120
  registro 69
  selecionando software 114
comandos
  HALT 157
  REPAIR STGPOOL 172
comunicações entre o servidor e o cliente
  configurando 125
comunicações seguras
  configurar com SSL e TLS 60
configuração
  alterando 128
  clientes 121
configuração de armazenamento
  planejando 13
configurando
  clientes 69
  servidor spoke 107
conformidade da licença
  verificando 101
conjunto de armazenamentos
  proteção 144
  reparar 144, 172
conjuntos de armazenamentos
  auditando contêineres 137

D

dados
  desativando 134
deduplicação de dados
  configurar o 65
deficiência 175
diretórios do IBM Spectrum Protect
  planejando 13
domínios de política
  especificando 115
drill de recuperação 165

E

E/S de caminhos múltiplos
  configurar para sistemas AIX 45
  configurar para sistemas Linux 46
  configurar para sistemas Windows 47
Encerrando
  server 157
espaço de armazenamento
  liberando 134

F

firewall 30, 31
firewalls
  configurando comunicações através de 125

G

gerenciando
  administradores 152
  autoridade 152
  níveis de acesso 154
gerenciando a segurança 149

H

hardware de armazenamento
  configurar o 37

I

IBM Knowledge Center v

ID de usuário
  criar para o servidor 48
implementação
  operações de teste 79
indisponibilidade
  preparar 163
iniciando o servidor
  modo de manutenção 157
instalação
  clientes 69, 121
instalação de servidor
  Sistemas AIX 53, 54
  Sistemas Linux 53, 54
instalando o sistema operacional
  sistemas do servidor AIX 38
  sistemas do servidor Linux 39
  sistemas do servidor Windows 44
instalar servidor
  Sistemas AIX 53
  Sistemas Linux 53

K

Knowledge Center v

L

LDAP
  requisitos de senha 153
licença do produto
  registro 64
licenciamento da unidade de valor do processador (PVU) 101
licenciamento de capacidade back-end 101
licenciamento de capacidade front-end 101
lista de verificação diária de tarefas de monitoramento 83
lista de verificação periódica de tarefas de monitoramento 93
logs de erro
  avaliando 127

M

manutenção
  definir planejamento 66
método de recuperação
  indisponibilidade do sistema 167
  perda de dados 167
modo de manutenção
  iniciar o servidor 157
monitoramento
  lista de verificação diária 83
  lista de verificação periódica 93
  objetivos 81
  tarefas
    lista de verificação diária 83
    lista de verificação periódica 93

N

nível de autoridade 152
nós clientes
  desatribuindo 132
  removendo da produção 132

O

opcionais
  configurar para o servidor 59
operações de archive
  especificando regras 115
  planejando 119
operações de backup
  especificando regras 115
  modificando o escopo 130
  planejando 119
Operations Center
  comunicações seguras 62
  configurar o 61
  restaurar para o estado pré-configurado 111
  servidor da web 109
  servidor spoke 107

P

parada (halt)
  server 157
parando
  server 157
perda de dados 167
planejamentos
  operações de backup e archive 119
planejando soluções
  disco multisite 1
planilha de planejamento 13
políticas
  editando 117
  especificando 115
  visualizando 117
problemas
  diagnosticando 81
processo de desativação
  dados de backup 134
processo de desatribuição
  nó cliente 132
publicações v

R

recuperação
  estratégia 165
  recuperação de desastre 165
recuperação de dados 163, 165, 167
  estratégia 165
recuperar arquivos danificados
  replicação 171
recursos de acessibilidade 175
registro
  clientes 120
regras
  editando 117
  especificando
    operações de backup e archive 115
  visualizando 117
regras de retenção de dados
  define 65
relatórios
  email
    configurando 103
relatórios de e-mail
  configurando 103

relatórios de status
  obtendo 103
reparar conjunto de armazenamentos
  danificado 172
replicação 77, 144
  ativando 143
  gerenciando 143
  modificando 146
  políticas do servidor de destino 147
  solução de disco multisite
    compatibilidade 143
replicação de nó
  ativar 77
requisitos de hardware 7
requisitos de memória
  gerenciando 140
requisitos de senha
  LDAP 153
Requisitos de Software
  Linux 9
requisitos do sistema 7, 9
  hardware 7
resolução de problemas 81
  erros em operações do cliente 126
  IDs de administrador 129
  nós clientes bloqueados 129
  problemas de senha 129
restringindo
  acesso de usuário 154

S

segundo servidor
  configurar o 75
  incluir como spoke 77
segurança 149
senhas
  alterando 153
  reconfigurando 129
server
  configurar o 57
  configurar o segundo servidor 75
  configurar opções 59
  criar ID do usuário para 48
  definir planejamento de manutenção 66
  iniciar no modo de manutenção 157
  parada 157
  planejar upgrade 161
serviço de gerenciamento de cliente
  configurar o Operations Center para usar 72
  instalação 70
  verificar instalação 71
servidor
  ativando a replicação 143
  ativando políticas do destino de replicação 147
  determinar o tamanho de 3
  gerenciando a replicação 143
  modificando a replicação 146
  recuperação de dados 171
  replicação de nó 143
servidor da web
  parada 109
  start 109
servidor de instalação
  Sistemas Windows 54
servidor do hub
  alterando 110
servidor do hub *(continuação)*
  comunicações SSL seguras 75
  restaurar para o estado pré-configurado 111
servidor spoke
  incluindo 107
  incluir 77
  Remover 108
servidores
  iniciar no modo de manutenção 158
servidores spoke
  restaurar para o estado pré-configurado 111
sistema operacional
  instalar em sistemas de servidor AIX 38
  instalar em sistemas de servidor Linux 39
  instalar em sistemas de servidor Windows 44
  segurança 154
sistemas de arquivos
  [preparando, sistemas de servidor AIX 49
  planejando 13
  preparando, sistemas de servidor Linux 50
  preparando, sistemas de servidor Windows 51
Sobre esta publicação v
software
  selecionando 114
solução
  expandindo 113
solução de disco multisite
  planejando 1
SSL 60
status do sistema
  rastreando 103

T

tarefas de manutenção
  iniciar o servidor no modo de manutenção 158
  planejando 141
tarefas de reconfiguração
  iniciar o servidor no modo de manutenção 158
teclado 175
TLS 60

U

upgrade
  server 161
uso do processador 140

Número do Programa: 5725-W98
5725-W99
5725-X15

Impresso no Brasil