

IBM Spectrum Protect  
Versão 8.1.0

## *Guia de Determinação de Problema*





IBM Spectrum Protect  
Versão 8.1.0

## *Guia de Determinação de Problema*



**Nota:**

Antes de usar estas informações e o produto que elas suportam, leia as informações em “Avisos” na página 227.

Esta edição se aplica à versão 8, liberação 1, modificação 0 do IBM Spectrum Protect (número do 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.

© Copyright IBM Corporation 1993, 2016.

---

# Índice

## Sobre esta Publicação . . . . . vii

Quem Deve Ler este Guia . . . . . vii

Publicações . . . . . vii

## Capítulo 1. Recursos da Ajuda . . . . . 1

Ajuda do Cliente de Backup-archive . . . . . 1

Ajuda de acesso para o Utilitário de configuração  
de serviço do cliente (**dsmcutil**) . . . . . 2

Ajuda do Servidor ou do Agente de Armazenamento 2

Acessando a Ajuda para Comandos do Servidor  
ou do Agente de Armazenamento . . . . . 2

Acessando a Ajuda para Mensagens . . . . . 3

Ajuda da Interface da Linha de Comandos para o  
Cliente . . . . . 3

Relatando um Problema com um Tópico da Ajuda. 3

## Capítulo 2. Resolvendo Problemas do Cliente . . . . . 5

Examinando Mensagens de Erro. . . . . 5

Examinando as Mensagens do Log de Atividades do  
Servidor . . . . . 5

Identificando quando e onde o Problema Pode  
Ocorrer . . . . . 5

Reproduzindo o Problema . . . . . 6

Coletando a Documentação para Resolver Problemas  
com o Aplicativo Cliente . . . . . 6

Determinando por que os programas **dsmc**, **dsmadm**,  
**dsm** ou **dsmj** não são iniciados. . . . . 7

Resolvendo Problemas com Conjuntos de Opções do  
Cliente . . . . . 9

Cenários para Resolver os Problemas com  
Conjuntos de Opções do Cliente. . . . . 9

Resolvendo Problemas de Expiração de Senha. . . 10

Resolvendo Problemas de Senha Autenticada por  
LDAP . . . . . 11

Verificando a Configuração de Autenticação de  
Senha . . . . . 11

O Servidor IBM Spectrum Protect não Aceita o  
LDAPPASSWORD . . . . . 12

Resolvendo Problemas com o Servidor de  
Diretório LDAP . . . . . 13

Auditando o Servidor de Diretório LDAP para  
Limpar o Servidor . . . . . 14

Mensagens de Erro para Senhas Autenticadas por  
LDAP . . . . . 15

Resolvendo Problemas de Planejamento de Cliente 18

Determinando o Status de um Evento Planejado 18

Verificando Erros no Log de Atividades do  
Servidor . . . . . 19

Iniciando e Parando o Serviço do Cliente . . . 20

Resolvendo Erros ao Incluir ou Excluir Arquivos de  
Cliente durante o Processo de Backup . . . . . 21

Identificando Arquivos que Foram Incluídos ou  
Excluídos pelo Conjunto de Opções do Cliente  
do Servidor . . . . . 21

Excluindo Arquivos Automaticamente do

Processo de Backup. . . . . 22

Excluindo Arquivos com a Instrução

EXCLUDE.DIR . . . . . 24

Determinando se as Instruções de Compactação,  
Criptografia ou de Backup de Subarquivo São de

Inclusão ou de Exclusão . . . . . 26

Usando Delimitadores para Incluir ou Excluir

Arquivos . . . . . 26

Resolvendo Problemas Devido à Codificação

Incorreta da Lista de Inclusão ou Exclusão . . . 27

Resolvendo Problemas de Diferença de Captura

Instantânea . . . . . 27

Resolvendo Problemas no Diretório de Captura

Instantânea para Volumes do Sistema de  
Arquivos NetApp ou N-Series . . . . . 30

Resolvendo Problemas de Login ao Usar o

Sistema de Arquivos com Criptografia nos

Sistemas Operacionais AIX . . . . . 30

Resolvendo Erros de Backup de Imagem . . . . . 31

Resolvendo Erros de Backup de Imagem do

Linux . . . . . 31

Resolvendo Falhas de Backup Ao Usar o Backup

de Imagem de Captura Instantânea Linux . . . 32

Resolvendo Erros durante o Backup-archive e

Backup de Imagem Baseados em Captura

Instantânea de JFS2 do AIX . . . . . 33

Soluções de Suporte para a API do IBM Spectrum

Protect . . . . . 35

Reunindo Informações da API antes de Entrar

em Contato com o Suporte IBM . . . . . 35

Coletando arquivos de API antes de chamar o

suporte do IBM . . . . . 36

Determinando se os dados são enviados para o

agente de armazenamento, em vez de para o

servidor . . . . . 38

Executando aplicativos que usam a API como ID do

usuário não raiz. . . . . 39

Determinação de Problemas do Journal Based

Backup . . . . . 41

Determinando se um Backup Será Baseado em

Diário . . . . . 42

Executando o Daemon de Diário em Primeiro

Plano . . . . . 43

O utilitário Journal Database Viewing . . . . . 43

Usando o Windows Volume Shadow Copy Services 45

Definindo Erros Temporários do VSS. . . . . 45

Definindo Sinalizadores de Teste de VSS do

Windows . . . . . 46

Ajuste de Volume Shadow Copy Services . . . 46

Reunindo Informações de Diagnóstico do VSS

para a Assistência Microsoft . . . . . 47

Resolvendo Erros Usando um Rastreamento do VSS 47

Executando Chamadas da API do VSS com o

Programa de Amostra vsreq.exe . . . . . 48

Comparando a Interação do IBM Spectrum Protect e do Ntbackup.exe com o VSS . . . . .	48
Comandos <b>SHOW</b> para o Cliente de Backup-Archive . . . . .	48
Resolvendo problemas para recuperação de bancos de dados Microsoft SQL individuais a partir de um backup de máquina virtual . . . . .	50
Resolvendo Problemas de Acesso ao Banco de Dados . . . . .	51
Visualizando Cópias Ativas de Bancos de Dados Microsoft SQL . . . . .	52
Bancos de Dados Microsoft SQL com Nomes DBCS . . . . .	52
Respostas para Mensagens de Backups da Máquina Virtual com Proteção de Aplicativo . . . . .	53
Salvando Arquivos de Manifesto VSS XML . . . . .	53
Determinando se um Backup de Máquina Virtual Pode Falhar . . . . .	54

### Capítulo 3. Resolvendo problemas do servidor IBM Spectrum Protect . . . . . 57

Recriando o Problema . . . . .	57
Verificando o arquivo de log de atividade do servidor e outros arquivos de log . . . . .	57
Verificando Erros de Dispositivo em Arquivos de Log de Erro de Sistema . . . . .	58
Revertendo Opções ou Configurações do Servidor . . . . .	58
Reiniciando o Serviço de Planejamento . . . . .	59
Resolvendo Problemas de Espaço do Servidor . . . . .	59
Alocando Memória Adicional do Servidor . . . . .	59
Configurando uma Instância do Servidor para Usar Memória Compartilhada . . . . .	60
Alterando a Frequência de Cópia . . . . .	61
Resolvendo Erros de Operação RELABEL . . . . .	61
Evitando Erros de Comunicação Durante o Processamento de Importação . . . . .	62
Incluindo um certificado autoassinado para o keystore . . . . .	62
Determinando por que os registros de resumo para um evento de backup do cliente estão ausentes . . . . .	63
Resolvendo Problemas de Instalação e Upgrade . . . . .	64
Arquivos de Log de Instalação . . . . .	64
O Assistente de Instalação Falha ao Iniciar . . . . .	65
Resolvendo Problemas de Instalação de GSKit . . . . .	65
Instâncias de Serviço Não Criadas Durante um Upgrade . . . . .	66
Resolvendo um Processo de Desinstalação Interrompido . . . . .	67
A Implementação Automática do Cliente não Fez Upgrade do Software Cliente . . . . .	67
Resolvendo Interrupções do Servidor . . . . .	68
Resolvendo uma Interrupção ou Loop . . . . .	69
Resolvendo Problemas de Estado de Espera com Servidores de Repositório do Usuário Externo . . . . .	70
Localizando o Arquivo de Erros do Servidor (dsmerv.err). . . . .	70
Localizando a Imagem do Sistema (Arquivo de Núcleo). . . . .	71
Recuperando Arquivos da Biblioteca para Análise Principal . . . . .	72
Recuperando Arquivos de Log do Sistema . . . . .	72
Recuperando o Log de Atividades . . . . .	73

Detectando Erros Após o Início e Parada do Serviço de Servidor . . . . .	73
O Diretório sqllib/db2dump Causa Encerramento . . . . .	73
Resolvendo problemas com a verificação de página do banco de dados . . . . .	75
Resolvendo Erros do Banco de Dados . . . . .	75
Resolvendo Problemas de Inicialização do Gerenciador de Banco de Dados . . . . .	75
Rastreando o plug-in ID de usuário e senha . . . . .	77
Limitando a Alocação de Memória do DB2 . . . . .	78
Recuperando Informações da Versão do DB2 . . . . .	78
Localizando os Arquivos de Log de Diagnóstico do DB2 . . . . .	79
Arquivos de Log de Upgrade do DB2 . . . . .	80
Resolvendo um Problema de ID do Banco de Dados Ausente ou Incorreto . . . . .	80
Resolvendo Problemas com os Comandos <b>BACKUP DB</b> e <b>RESTORE DB</b> . . . . .	81
Características do ID do Usuário \$\$_TSMDBMGR_\$\$ . . . . .	86
Resolvendo Problemas de Reorganização de Banco de Dados . . . . .	86
Analisando os Sintomas do Processo para Resolver Problemas . . . . .	87
Revisando as Mensagens do Processo para Determinar o Estado de Operações do Servidor . . . . .	87
Analisando a Mensagem de Erro ANR1221E . . . . .	93
Analisando a Mensagem de Erro ANR2317W . . . . .	94
Analisando as Mensagens de Erro ANR1330E e ANR1331E. . . . .	95
Os Arquivos Não Expiram após a Redução de Versões . . . . .	98
Os Sintomas do Processo Indicam Erros de Migração . . . . .	99
Resolvendo Problemas do Conjunto de Armazenamentos . . . . .	99
Recebida a Mensagem “ANR0522W Falha na transação...” . . . . .	100
O Conjunto de Armazenamentos Têm Alto Uso de Volume após o Aumento do Valor <b>MAXSCRATCH</b> . . . . .	101
O conjunto de armazenamentos está configurado para usar disposição, mas os volumes contêm dados que não estão dispostos . . . . .	101
Resolvendo Problemas de Armazenamento dos Conjuntos de Dados Ativos. . . . .	102
Resolvendo problemas com conjuntos de armazenamentos de contêiner em nuvem . . . . .	103

### Capítulo 4. Resolvendo Problemas do Operations Center . . . . . 105

Visão geral de arquivos de log . . . . .	105
Visualizando o log do Operations Center a partir do Operations Center . . . . .	106
Alertas não São Atualizados Imediatamente . . . . .	106
Tarefas Ativas não São Canceladas Imediatamente . . . . .	107
Problemas Adicionais Conhecidos com o Centro de Operações . . . . .	108

## Capítulo 5. Resolvendo Problemas de Comunicação . . . . . 109

Resolvendo Erros Criados ao Conectar-se ao Servidor . . . . .	109
Resolvendo Conexões com Falha por Clientes ou Administradores . . . . .	109
Resolvendo Erros de Secure Sockets Layer. . . . .	110
Recuperando a Senha do Arquivo de Banco de Dados de Chaves . . . . .	112
Resolução de problemas do banco de dados da chave do certificado . . . . .	113

## Capítulo 6. Resolvendo Problemas do Agente de Armazenamento . . . . . 115

Verificando o Log de Atividades do Servidor para Obter Informações do Agente de Armazenamento . . . . .	115
Resolvendo um Erro Causado por Leitura ou Gravação em um Dispositivo . . . . .	115
Resolvendo Problemas Causados pela Mudança de Opções do Agente de Armazenamento . . . . .	116
Resolvendo Problemas Causados pela Mudança de Opções ou Configurações do Servidor . . . . .	116
Configuração sem a LAN do Agente de Armazenamento . . . . .	116
Resolvendo o Problema de Envio de Dados Diretamente para o Servidor . . . . .	116
Resolvendo um Conjunto de Armazenamento Ativado Sem a LAN Desqualificado . . . . .	118
Assegurando que os Dados Sejam Transferidos Usando um Ambiente sem a LAN . . . . .	118

## Capítulo 7. Usando o Rastreio para Resolver Problemas . . . . . 119

Iniciando um rastreio estendido do Operations Center. . . . .	119
Rastreando o Operations Center ativando funções de criação de log a partir do Operations Center. . . . .	119
Rastreando o Operations Center ativando funções no arquivo de configuração de criação de log . . . . .	120
Ativando um Rastreio para o Servidor ou Agente de Armazenamento . . . . .	121
Ativando um Rastreio de Pilha para Mensagens para o Servidor ou Agente de Armazenamento . . . . .	123
Classes de Rastreio para um Servidor ou Agente de Armazenamento . . . . .	124
Comandos Show para o Servidor e o Agente de Armazenamento . . . . .	140
Ativando um Rastreio para o Driver de Dispositivo do IBM Spectrum Protect . . . . .	150
Rastreio a partir do Console do Servidor . . . . .	150
Rastreando dados a partir de um shell de comando para AIX e Windows . . . . .	152
Rastreio para Detectar uma Falha de Conversão de Página de Códigos . . . . .	152
Dados de Rastreio para o Cliente. . . . .	152
Sinalizadores de Rastreio do Cliente e do Daemon de Diário. . . . .	154
Classes de Rastreio do Cliente. . . . .	154

Ativando o Rastreio do Cliente de Backup-archive . . . . .	160
Determinando se os dados são criptografados ou compactados durante o archive de backup usando rastreio. . . . .	170
Dados de Rastreio para a API . . . . .	171
Rastreando o Agente do Tivoli Monitoring for Tivoli Storage Manager em um Sistema AIX ou Linux . . . . .	172
Rastreando o Agente do Tivoli Monitoring for Tivoli Storage Manager em um Sistema Operacional Windows . . . . .	174

## Capítulo 8. Resolvendo Problemas de Armazenamento de Dados. . . . . 177

Resolvendo Problemas de Dados Ilegíveis . . . . .	177
Verificando o Log de Atividades do Servidor para Resolver Problemas de Armazenamento de Dados . . . . .	177
Verificando em HELP Mensagens Emitidas para um Problema de Armazenamento de Dados . . . . .	177
Recriando o Problema de Armazenamento de Dados . . . . .	178
Resolvendo Erros de Armazenamento de Dados Relacionados à Leitura ou Gravação em um Dispositivo . . . . .	178
Alterando a Hierarquia de Armazenamento para Resolver Problemas de Armazenamento de Dados . . . . .	178
Alterando as Políticas do Servidor para Resolver Problemas de Armazenamento de Dados . . . . .	179
Resolvendo um Problema de Backup ou Cópia de Armazenamento de Dados que Ocorre apenas com um Nó Específico . . . . .	179
Resolvendo um Problema de Armazenamento de Dados que Ocorre apenas para um Volume Específico . . . . .	180
Sugestões e Dicas de Armazenamento . . . . .	180
Sugestões e Dicas do Driver de Dispositivo . . . . .	180
Sugestões e Dicas de Unidades de Disco Rígido e de Subsistemas de Disco . . . . .	185
Sugestões e Dicas de Unidades e Bibliotecas de Fitas . . . . .	188
Dicas e Sugestões de SAN . . . . .	190
Sugestões e Dicas de Operações do Arquivador NDMP para o Servidor IBM Spectrum Protect . . . . .	205
Resolvendo Problemas do Dispositivo SCSI . . . . .	206
Resolvendo Erros de Volume de Mídia Sequencial (Fita) por meio das Mensagens ANR0542W ou ANR8778W . . . . .	207

## Apêndice A. Obtendo Informações da Pilha de Chamada de um Arquivo Principal . . . . . 209

## Apêndice B. Executando o Utilitário tsmdiag . . . . . 211

Opções do utilitário tsmdiag . . . . .	212
--	-----

<b>Apêndice C. Códigos de Retorno do IBM Global Security Kit . . . . .</b>	<b>213</b>
--	------------

<b>Apêndice D. Recursos de Acessibilidade para a Família de Produtos IBM Spectrum Protect . . .</b>	<b>225</b>
---	------------

<b>Avisos . . . . .</b>	<b>227</b>
-------------------------	------------

<b>Glossário . . . . .</b>	<b>231</b>
----------------------------	------------

<b>Índice Remissivo . . . . .</b>	<b>233</b>
-----------------------------------	------------



---

## Sobre esta Publicação

Esta publicação o ajuda a determinar a origem dos problemas com os servidores e clientes no ambiente do IBM Spectrum Protect.

Antes de usar esta publicação, certifique-se de estar familiarizado com as seguintes áreas:

- Os sistemas operacionais do cliente e do servidor IBM Spectrum Protect
- Os protocolos de comunicação que estão instalados em seus computadores cliente e servidor

---

## Quem Deve Ler este Guia

Este guia é escrito para qualquer pessoa que administra ou gerencia o IBM Spectrum Protect. De modo semelhante, as informações fornecidas por esse guia podem ser úteis para parceiros de negócios e para qualquer pessoa com responsabilidade no suporte do IBM Spectrum Protect.

Você deve estar familiarizado com o IBM Spectrum Protect e os sistemas operacionais usados para o ambiente do IBM Spectrum Protect.

---

## Publicações

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

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



---

## Capítulo 1. Recursos da Ajuda

O IBM Spectrum Protect possui várias opções para a resolução de problemas que você possa ter com o servidor ou com o cliente de backup-archive.

---

### Ajuda do Cliente de Backup-archive

Use o comando `help` para exibir informações sobre comandos, opções e mensagens. Se você usar o comando `help` na linha de comandos inicial, nenhum contato com o servidor será feito e nenhuma senha será necessária.

#### Sintaxe

```
➤—dsmc help—➤
├—command-name [subcommand-name]—
├—option-name—
├—TOC-section-number—
└—[ANS]message-number—
```

Digitar o comando **HELP** sem argumentos faz com que a ajuda exiba o índice completo. Seja com o comando inicial ou quando **HELP** exibe um prompt, você pode digitar os parâmetros a seguir.

#### Parâmetros

*command-name [subcommand-name]*

Especifica um nome de comando e, opcionalmente, um nome de subcomando ou sua abreviação. Por exemplo: **backup image**, ou **b i**. Nesse caso, a combinação deve ser exclusiva. Abreviações não exclusivas resultam na exibição da primeira seção do arquivo de ajuda inteiro correspondente a elas. Este parâmetro é opcional.

*option-name*

Especifica o nome de uma opção. Por exemplo: `domain` ou `do`. Este parâmetro é opcional.

*TOC-section-number*

Especifica o número da seção de índice. Por exemplo: 1.5.3. Este parâmetro é opcional.

*[ANS]message-number*

Especifica um número de mensagem com ou sem seu prefixo. Por exemplo: `ans1036` ou `1036`. Este parâmetro é opcional. O código de gravidade nunca é necessário. A inserção de `ans1036E` resulta em uma resposta não localizada.

**Importante:** Se você inserir argumentos que não se adequam a essas descrições, resultados inesperados (ou nenhum resultado) poderão ser exibidos. Se você inserir mais de dois argumentos, seu pedido de ajuda será rejeitado. Quando os nomes de um comando e de uma opção forem iguais, por exemplo: **incremental** (comando) e **incremental** (opção), a ajuda para a opção só poderá ser obtida digitando-se seu número de sessão do índice.

O texto de ajuda solicitado é exibido em uma ou mais seções, dependendo do número de linhas de exibição que estão disponíveis em sua janela de comando.

Quando linhas suficientes forem exibidas para preencher o espaço de exibição ou quando o final do texto de ajuda solicitado for exibido, um prompt será apresentado com instruções sobre o que pode ser inserido nesse prompt. Para continuar exibindo texto para sua seleção atual, pressione **Enter** ou pressione a tecla “d” para rolar para baixo. Para rolar para cima na seleção atual, pressione a tecla “u” e pressione **Enter**. Use a tecla “q” para encerrar o recurso da ajuda. Outras opções podem ser apresentadas, portanto, leia todas as instruções.

Uma exibição apropriada do texto de ajuda requer uma largura de exibição utilizável de 72 caracteres. Uma exibição com largura inferior a 72 caracteres faz com que as frases com mais de 72 caracteres sejam quebradas para a próxima linha. Isso pode fazer com que o texto de ajuda exibido comece em algum lugar dentro da seção que não seja no começo. As linhas que não são exibidas podem ser visualizadas usando a função de rolagem do terminal para mover para cima.

## Ajuda de acesso para o Utilitário de configuração de serviço do cliente (`dsmcutil`)

Windows

Para obter informações da ajuda para o Utilitário de Configuração de Serviço do Cliente IBM Spectrum Protect, você deve emitir o comando **DSMCUTIL HELP**.

Ao emitir o comando **DSMCUTIL HELP**, as informações de ajuda são exibidas no utilitário de ajuda Windows.

---

## Ajuda do Servidor ou do Agente de Armazenamento

O servidor e agente de armazenamento incluem um recurso de ajuda. Esse recurso de ajuda fornece descrições e sintaxe de comandos do servidor e uma descrição completa de mensagens do servidor.

## Acessando a Ajuda para Comandos do Servidor ou do Agente de Armazenamento

Emita o comando **HELP** para acessar a ajuda do servidor ou agente de armazenamento.

Para exibir a ajuda da linha de comandos dos comandos do servidor que possuem nomes exclusivos, você pode digitar `help commandName`, em que *commandName* é o nome do comando do servidor do qual você deseja informações. Por exemplo, para exibir ajuda para o comando **REGISTER NODE**, digite `help register node`. A sintaxe do comando e as descrições de parâmetros são exibidas na saída.

Você também pode digitar `help` seguido pelo número do tópico do comando. Números de tópicos são listados no índice da ajuda da linha de comandos, por exemplo:

```
3.0
Administrative commands
  3.46
  REGISTER
    3.46.1 REGISTER ADMIN (Register an administrator)
    3.46.2 REGISTER LICENSE (Register a new license)
    3.46.3 REGISTER NODE (Register a node)
```

Para exibir ajuda sobre o comando **REGISTER NODE**, digite:

```
help 3.46.3
```

Use os números de tópicos para exibir a ajuda da linha de comandos para subcomandos. **DEFINE DEVCLASS** é um exemplo de um comando que possui subcomandos. Por exemplo, é possível especificar o comando **DEFINE DEVCLASS** para classes de dispositivo 3590 e para classes de dispositivo 3592:

```
3.0
Administrative commands
...
3.13.10 DEFINE DEVCLASS (Define a device class)
3.13.10.1 DEFINE DEVCLASS (Define a 3590 device class)
3.13.10.2 DEFINE DEVCLASS (Define a 3592 device class)
...
```

Para exibir ajuda para o comando **DEFINE DEVCLASS** para as classes de dispositivos 3590, digite:

```
help 3.13.10.1
```

## Acessando a Ajuda para Mensagens

Emita o comando de ajuda para acessar a ajuda das mensagens.

Emita o seguinte comando para obter ajuda sobre uma mensagem do servidor: **HELP *message number*** em que *message number* é a mensagem para a qual você deseja obter informações. Se você especificar o número da mensagem sem incluir o prefixo da mensagem, por exemplo, **HELP 0445**, ele assumirá o prefixo da mensagem ANR e relatará as informações da ajuda para ANR0445W. Se o número da mensagem for especificado com o prefixo, por exemplo **HELP ANR0445**, as informações de ajuda dessa mensagem serão relatadas. Emita **HELP ANR0445** para visualizar a seguinte saída de exemplo para essa mensagem:

```
ANR0445W Erro de protocolo no número da sessão para o nome do nó do cliente do nó
(plataforma do cliente) - excedido o tamanho máximo da transação do grupo.
Explicação: O servidor detecta um erro de protocolo na sessão especificada
porque o cliente tentou agrupar mais do que o máximo de operações de atualização
do banco de dados em uma única transação do banco de dados.
Ação do Sistema: O servidor termina a sessão do cliente.
Resposta do Usuário: Corrija o erro de programação no programa cliente, se ele
tiver sido gravado por sua instalação usando verbos WDSF. Caso contrário, entre
em contato com o seu representante de serviço.
```

## Ajuda da Interface da Linha de Comandos para o Cliente

A interface do cliente da linha de comandos inclui um recurso de ajuda que fornece descrições e a sintaxe de comandos e opções do cliente e uma descrição completa das mensagens do cliente.

As informações de ajuda da interface gráfica com o usuário (GUI) e dos clientes da GUI da web estão disponíveis no item de menu **Ajuda**.

---

## Relatando um Problema com um Tópico da Ajuda

Quando você deseja relatar um problema com o sistema de ajuda, primeiro deve coletar informações específicas.

1. Grave o que você clicou para obter ajuda. Por exemplo, se você clicou no ponto de interrogação para um portal, registre o nome do portal.
2. Visualize a origem da janela pop-up da ajuda. Na maioria dos navegadores, um clique no botão direito do mouse mostra um menu com a opção **Visualizar Origem**. Selecione **Visualizar Origem** para visualizar o código fonte HTML

daquela janela. Anote o título dessa janela, que é a URL ou o nome do arquivo que o sistema de ajuda está tentando mostrar.

---

## Capítulo 2. Resolvendo Problemas do Cliente

A resolução de problemas com o aplicativo cliente pode envolver a conexão com o servidor, a mudança de configurações de política, a reprodução do erro ou várias outras opções possíveis.

---

### Examinando Mensagens de Erro

É possível examinar as mensagens de erro geradas durante a operação do programa para ajudá-lo a resolver problemas que possam ocorrer.

Se estiver configurada, a opção Cliente IBM Spectrum Protect QUIET vai suprimir a exibição de todas as mensagens na saída de tela. No entanto, todas as mensagens ainda possuem login efetuado nos arquivos de log. Desligar a opção QUIET pode facilitar as operações de resolução de problemas porque você pode ver as mensagens na tela, conforme ocorrerem.

Procure por quaisquer mensagens ANSnnnnx que forem emitidas para o console. As mensagens também são registradas. As mensagens do planejador são registradas no arquivo dsm sched.log. As mensagens do cliente são registradas no arquivo dsmerror.log. Descrições das mensagens e códigos de retorno de API são fornecidos em Mensagens, Códigos de Retorno e Códigos de Erro. A ajuda online também está disponível para mensagens do sistema. Para obter ajuda online para uma mensagem quando você estiver usando o cliente de linha de comandos, digite **HELP ANS\_nnnnx**, em que *nnnn* é o número da mensagem e *x* é o tipo da mensagem.

---

### Examinando as Mensagens do Log de Atividades do Servidor

Use o comando **QUERY ACTLOG** para visualizar o arquivo de log de atividade do servidor e as mensagens emitidas para esta sessão do cliente.

As mensagens do log de atividades do servidor podem fornecer informações adicionais sobre os sintomas para o problema ou podem fornecer informações sobre a causa real do problema encontrado pelo cliente.

---

### Identificando quando e onde o Problema Pode Ocorrer

Problemas com o processamento do cliente geralmente ocorrem quando você está executando operações específicas, em determinados momentos, ou apenas em determinados clientes.

Para isolar ainda mais quando e onde um problema ocorre, determine as seguintes respostas:

- Este problema ocorre para um único cliente, para alguns clientes ou para todos os clientes para um determinado servidor?
- Este problema ocorre para todos os clientes em execução em um sistema operacional específico?
- Este problema ocorre para arquivos específicos, para arquivos que estão em um diretório específico, para arquivos em uma unidade específica ou para todos os arquivos?

- Este problema ocorre para clientes em uma rede, sub-rede específica ou em todas as partes da rede?
- Este problema ocorre apenas para o cliente da linha de comandos, para o cliente da GUI ou para o cliente da web?
- O IBM Spectrum Protect sempre falha ao processar o mesmo arquivo ou diretório, ou é diferente de execução para execução?

---

## Reproduzindo o Problema

Ao reproduzir um problema como parte da determinação de problema, tente minimizar o impacto que o processo tem sobre o IBM Spectrum Protect.

É possível ajudar o suporte do IBM Spectrum Protect minimizando a complexidade do ambiente no qual você deseja recriar o problema. As seguintes opções podem ser usadas para minimizar a complexidade do ambiente:

- Use um arquivo de opções mínimo consistindo apenas em TCPSEVERADDRESS, TCPPEORT e NODENAME.
- Se o problema ocorrer para um arquivo durante um backup incremental, tente reproduzir o problema com um backup seletivo apenas desse arquivo.
- Se o problema ocorrer durante um evento planejado, tente reproduzir o problema executando manualmente o comando.

---

## Coletando a Documentação para Resolver Problemas com o Aplicativo Cliente

A equipe de suporte IBM será capaz de resolver melhor um problema se for possível fornecer a eles a documentação relevante. O cliente de backup-archive cria informações em diversas origens diferentes.

**Dica:** O IBM Spectrum Protect tem um recurso de ajuda integrado na linha de comandos do cliente. Emita o comando **dsmc help** para acessar o recurso de ajuda do cliente da linha de comando. O recurso da ajuda é uma interface acionada por menu com informações que incluem a referência de comando, referência de opção e informações estendidas sobre mensagens do cliente.

Informações de configuração e problemas do cliente podem ser localizados em um ou mais dos seguintes documentos:

- Log de erros. O arquivo do log de erros é `dsmerror.log`.
- Log do planejador. O log de erros para o planejador de cliente é `dsmsched.log`.
- Log do Web client. O log de erros do cliente da web é `dsmwebcl.log`.
- Arquivos de opções. As informações sobre as opções que você configura para os clientes podem facilitar o diagnóstico e resolução de problemas. Muitas dessas informações estão contidas nos arquivos a seguir:
  - O arquivo de opções do cliente (`dsm.opt`). Este arquivo existe para todos os clientes em todos os sistemas operacionais.
  - O arquivo de opções do sistema do cliente (`dsm.sys`). Este arquivo é usado somente nos clientes do AIX, Linux e Mac OS X.
  - O arquivo de inclusão-exclusão. Este arquivo contém os objetos para incluir ou excluir das operações do cliente. Seu local é configurado pela opção `incl excl` do cliente.
- Dados de rastreamento. Se o recurso de rastreamento estava ativo, o arquivo que contém os dados de rastreamento pode ser fornecido para suporte.



- Dump do aplicativo. Quando o cliente de backup-archive para de executar inesperadamente, muitas plataformas geram um dump de aplicativo. O sistema operacional fornece o dump do aplicativo.
- Dump de memória. Se o cliente de backup-archive parar, um dump de memória poderá ser gerado e então ser usado para ajudar com diagnóstico. O tipo de sistema determina como ocorre o dump de memória e o sistema operacional fornece o dump de memória.

O comando **DSMC QUERY SYSTEMINFO** está disponível e coleta a maioria dessas informações no arquivo `dsminfo.txt`. Os seguintes itens podem ajudá-lo a determinar problemas do IBM Spectrum Protect:

- Uma lista de todos os produtos de software instalados no sistema do cliente. O cliente pode ter problemas devido a interações com outro software no computador ou devido aos níveis de manutenção de software que o cliente usa.
- Conjuntos de opções do cliente que estão definidos no servidor que se aplicam a este nó cliente. Emita o comando **QUERY CLOPTSET** para procurar os conjuntos de opções do cliente.
- Opções do servidor. Inúmeras opções do servidor são usadas para gerenciar a interação entre o cliente de backup-archive e o servidor. Um exemplo dessa opção do servidor é `TXNGROUPMAX`.
- Informações sobre este nó conforme ele está definido no servidor. Para coletar estas informações, emit o comando **QUERY NODE *nodeName* F=D**, usando um cliente administrativo que está conectado ao servidor.
- Definições de planejamento para os planejamentos que se aplicam a este nó. As definições de planejamento podem ser consultadas do servidor quando você emite o comando **QUERY SCHEDULE**.
- As informações de política configuradas para esse nó no servidor. As informações de política podem ser consultadas do servidor quando você emite os comandos **QUERY DOMAIN**, **QUERY POLICYSET**, **QUERY MANAGEMENTCLASS** ou **QUERY COPYGROUP**.

---

## Determinando por que os programas `dsmc`, `dsmadmc`, `dsm` ou `dsmj` não são iniciados

O cliente de backup-archive usa os programas **dsmc**, **dsmadmc**, **dsm** ou **dsmj** em seu procedimento de inicialização. Quando um desses programas não inicia, o cliente de backup-archive não inicia.

Os programas **dsmc**, **dsmadmc**, **dsm** ou **dsmj** possuem as definições a seguir:

**dsmc** O cliente da linha de comando de backup-archive.

**dsmadmc**

O cliente da linha de comando administrativo.

Windows	<b>dsm</b>
AIX	Linux <b>dsmj</b>

A interface gráfica com o usuário (GUI) do cliente de backup-archive. A versão de runtime do Oracle Java™ é verificada quando você inicia pela primeira vez a GUI Java. Em alguns casos, esta verificação não é concluída corretamente e a inicialização de **dsm** ou **dsmj** pode falhar com uma mensagem de “número inválido”.

O processamento para e a mensagem a seguir é exibida, se o programa **dsmc**, **dsmadmc**, **dsm** ou **dsmj** não for iniciado:

ANS1398E As funções de inicialização não podem abrir um dos Logs do IBM Spectrum Protect ou um arquivo relacionado: dsmerror.log. errno = 13, As permissões de arquivo do arquivo não permitem a ação especificada.

**Lembre-se:** O arquivo dsmerror.log é usado apenas como um arquivo de exemplo na mensagem.

Os aplicativos clientes não são executados sem que sejam capazes de gravar em um arquivo de log e o sistema negar o acesso de gravação ao arquivo de log nomeado na mensagem. Se o arquivo de log não existir, ele será criado com as permissões padrão. As seguintes regras se aplicam:

1. O nome e o diretório que é especificado pela opção ERRORLOGNAME são usados.
2. Se a opção estiver ausente, será usado o nome dsmerror.log no diretório que é especificado na variável de ambiente **DSM\_LOG**, se presente. Caso contrário, será usado o nome dsmerror.log no diretório de trabalho atual.

Os seguintes problemas serão aplicáveis se forem usadas as permissões padrão:

- Um arquivo de log que é criado pelo usuário root não pode ser gravado por nenhum outro usuário
- O usuário root deve configurar as permissões ou listas de controle de acesso (ACLs) apropriadas para permitir o uso livre do aplicativo cliente por todos os usuários que precisam usá-lo

Se o arquivo de log for criado com êxito, uma sessão sem erros deixará um arquivo de log com comprimento zero (vazio).

O cliente não tenta criar arquivos de log no diretório-raiz. A mensagem ANS1398E é exibida quando o método na primeira regra direciona o arquivo de log para ser criado no diretório raiz.

Se um arquivo de log existir e puder ser localizado, o IBM Spectrum Protect usará o método da primeira regra. Ele também pode estar no diretório raiz, se você escolher. Além disso, todas as permissões concedidas a esse arquivo de log serão preservadas pelo código do IBM Spectrum Protect.

Crie seu arquivo de log antes do primeiro uso, assegurando que todos os usuários elegíveis tenham acesso de gravação a ele. Defina a opção ERRORLOGNAME ou a variável de ambiente **DSM\_DIR** para designar seu arquivo de log predefinido.

**Atenção:** Um erro de arquivo de log do sistema indica que você não pode gravar no arquivo dsmerror.log. Certos aplicativos de plano de fundo IBM Spectrum Protect podem não ser iniciados devido a erros de gravação para o arquivo dsmerror.log. Quando ocorrem esses erros, diversos erros são gravados no arquivo de log de eventos do sistema Windows e no arquivo de log do sistema em outros sistemas operacionais.

**Windows** Por exemplo:

```
C:\Arquivos de Programas\Tivoli\Tsm\baclient>net start "TSM Sched"
O serviço de planejamento do servidor está sendo iniciado.
O serviço de planejamento do servidor não pôde ser iniciado.
Ocorreu um erro específico do serviço: 12.
```

**AIX**

**Linux**

**Mac OS X**

As etapas de configuração extra são necessárias para que usuários não root possam executar aplicativos do IBM Spectrum Protect

ou aplicativos do IBM Spectrum Protect para Data Protection. Você recebe o erro ANS1398E se tentar executar aplicativos IBM Spectrum Protect usando um arquivo de log de erro que já foi gerado por root, que foi deixado com permissões padrão. Para clientes de proteção de dados, você poderá receber somente um erro da API do IBM Spectrum Protect. A seguir está um método para configurar o dsmerror.log para uso por usuários não root:

1. Configure **ERRORLOGNAME** em dsm.sys. Por exemplo, errorLogName /var/msgs/tsm/dsmerror.log
2. Gere **dsmerror.log**. **dsmc q sess**
3. Modifique as permissões em dsmerror.log para permitir a gravação por todos os usuários. **chmod 666 /var/msgs/tsm/dsmerror.log**

---

## Resolvendo Problemas com Conjuntos de Opções do Cliente

Com conjuntos de opções do cliente, os administradores podem especificar opções adicionais que podem não estar incluídas no arquivo de opções do cliente de backup-archive. O cliente de backup-archive usa essas opções durante um processo de backup, archive, restauração ou recuperação.

Um administrador para o IBM Spectrum Protect pode criar um conjunto de opções do cliente a ser usado por um nó cliente no IBM Spectrum Protect. As opções do cliente são definidas no servidor IBM Spectrum Protect. As opções do cliente que são especificadas no conjunto de opções do cliente são usadas em conjunto com o arquivo de opções do cliente.

A ordem na qual as opções são processadas pode ser controlada. Várias opções podem ser definidas e depois um número de sequência pode ser designado com essas opções e depois processadas de uma sequência baixa para alta. O exemplo a seguir exhibe as opções **INCLEXCL**:

Opção	Sequência number	Substituição	Valor da Opção
-----	-----	-----	-----
INCLEXCL	0	No	exclude 'sys:\backup\*'
INCLEXCL	1	No	include 'sys:\system\*'
INCLEXCL	2	No	include 'sys:\tmp\*'

Essa sequência resulta na exclusão de todos os arquivos no caminho sys:\backup\\*, durante o backup dos arquivos nos caminhos sys:\system\\* e sys:\tmp\\*.

## Cenários para Resolver os Problemas com Conjuntos de Opções do Cliente

Use os conjuntos de opções do cliente para resolver vários problemas, de ter ambientes críticos nos quais a restauração é de alta prioridade a usar um banco de dados que não para.

**Dica:** As configurações de rastreamento dos conjuntos de opções do cliente são especificadas no arquivo de opções do IBM Spectrum Protect para todos os clientes de backup-archive.

Os seguintes cenários mostram como você pode se beneficiar do conjunto de opções do cliente.

### **Cenário 1: Tendo um ambiente no qual a restauração é uma alta prioridade.**

Use a opção COLLOCATEBYFILESPEC para que todos os dados de especificação de arquivo sejam armazenados como o mínimo de fitas possíveis, pois o uso de menos conjuntos de fitas aperfeiçoa o processamento de restauração. Você não deseja que o cliente substitua esta opção. Emita o seguinte comando do servidor:

```
Define cloptset crit_rest description="Critical Restore Option Sets"
Define clientopt crit_rest collocatebyfilespec yes force=yes
Update node dale cloptset=crit_rest
```

### **Cenário 2: Usando estações de trabalho que estão em uma rede lenta com espaço limitado para dados no servidor.**

Use a opção de compactação para limitar a quantia de dados que é enviada e armazenada. Emita o seguinte comando do servidor:

```
Define cloptset space_rest description="Space Restriction Option Sets"
Define clientopt space_rest compressalways no force=yes
Define clientopt space_rest compression yes force=yes
Update node mark cloptset=space_rest
```

### **Cenário 3: Usando um banco de dados que não para.**

Existe um problema com o banco de dados, pois os arquivos estão abertos e o servidor não pode fazer backup deles. Exclua todos os arquivos e subdiretórios dos backups do IBM Spectrum Protect e inclua os arquivos e subdiretórios no conjunto de opções do cliente "space\_rest" existente. Emita o comando **EXCLUDE DIR** e especifique o caminho de diretório que deve ser excluído. Emita o seguinte comando do servidor:

```
Define clientopt space_rest inclexcl "exclude.dir c:\notes\data"
```

### **Cenário 4: Concluindo backups usando uma rede rápida e aguardando para fazer o melhor uso possível de recursos do cliente.**

Configure a opção RESOURCEUTILIZATION para a quantidade máxima. Emita o seguinte comando do servidor:

```
Define cloptset unix_srv description="UNIX Server Option Sets"
Define clientopt unix_srv resourceutilization 10 force=yes
```

---

## **Resolvendo Problemas de Expiração de Senha**

Se você receber um erro de autenticação de cliente, ele pode ser o resultado de uma senha expirada. A expiração de senha não se aplica a senhas do nó ou do administrador que são autenticadas com um servidor de diretório LDAP.

### **Procedimento**

Conclua as seguintes etapas para alterar o período de senha expirada:

1. Para alterar o período de expiração da senha para um nó específico, emita o comando do servidor **UPDATE NODE** com a opção **PASSEXp=n**, em que *n* é o número de dias. Um valor 0 desativa a expiração de senha.

Se um nó cliente Windows não puder se conectar ao servidor após ser renomeado, verifique se o nome do nó foi alterado no arquivo de opções do cliente e no registro do Windows. Quando o planejador de cliente for executado como um processo em primeiro plano e usar o comando **DSMC SCHED**, o IBM

Spectrum Protect usará o nome do nó no arquivo de opções do cliente para entrar em contato com o servidor. No entanto, quando o planejador for executado como um serviço do Windows, o IBM Spectrum Protect usará o nome do nó no registro do Windows.

2. Para o cliente Windows, emita o comando **DSMCUTIL UPDATE SCHEDULE** para arquivar os resultados a seguir:
  - Com o parâmetro *node*, verifique como alterar o nome do nó que é usado com o serviço do planejador do IBM Spectrum Protect no Windows
  - Com o parâmetro *validate:yes*, entre em contato com o servidor IBM Spectrum Protect para autenticar (e armazenar a senha atualizada)

---

## Resolvendo Problemas de Senha Autenticada por LDAP

A maioria dos problemas que surgem de autenticação de senha podem ser atribuídos à conexão entre o servidor IBM Spectrum Protect e o servidor de diretório LDAP.

Esta documentação refere-se ao método de autenticação LDAP usado para servidores anteriores à V7.1.7 e pelos usuários do IBM Security Directory Server. Para obter mais informações sobre este método, consulte Senhas de gerenciamento e procedimentos de logon (V7.1.1)

Antes de usar a senha autenticada por LDAP, você deve configurar o servidor de diretório LDAP para comunicação com o servidor IBM Spectrum Protect. Certifique-se de que a lista de controle de acesso no servidor de diretório LDAP conceda autoridade plena a um usuário (LDAPUSER) sobre o nome distinto de base (DN Base).

## Verificando a Configuração de Autenticação de Senha

Se você configurou o servidor para autenticar senhas com um servidor de diretório LDAP e estiver recebendo erros, revise as etapas de configuração. Você deve assegurar que o servidor IBM Spectrum Protect e o servidor de diretório LDAP estejam configurados corretamente.

### Procedimento

1. Abra o arquivo de opções `dsmserv.opt` e localize a opção **LDAPURL**, que contém o servidor e o nome distinto de base (DN Base). É possível incluir mais valores na opção **LDAPURL**, com cada valor de URL tendo até 1024 caracteres. O número da porta é opcional. O número da porta padrão é 389. Cada configuração da URL deve conter os seguintes valores:
  - Um nome do servidor de diretório LDAP
  - O DN Base do namespace ou sufixo mantido pelo servidor de diretório LDAP. O formato do DN deve estar em conformidade com o servidor de diretório escolhido.

A opção **LDAPURL** deve estar de acordo com as seguintes especificações:

- Se você especificar diversas URLs, siga estas diretrizes:
  - Cada URL deve estar em uma linha separada
  - Cada URL deve apontar para um diretório externo diferente e todos os diretórios externos devem conter os mesmos dados
- Cada URL deve iniciar com o valor a seguir: `ldap://`

Por exemplo:

```
LDAPURL ldap://zapp.storage.dallas.gov/ou=tsmdata,dc=storage,dc=dallas,dc=com
```

A URL especificada não pode ser uma URL segura, o que significa que ela não pode começar com ldaps://.

2. Visualize as configurações de **LDAPUSER** ou **LDAPPASSWORD**, emitindo o comando **QUERY STATUS**. Defina o **LDAPUSER** que pode então incluir ou remover entradas, e alterar ou reconfigurar senhas. Se o **LDAPUSER** não estiver definido, emita o comando **SET LDAPUSER** para definir o administrador do servidor de diretório LDAP.

**Importante:** Se o valor para o parâmetro **LDAPUSER** inclui caracteres especiais, coloque o valor entre aspas. Por exemplo:

```
set ldapuser "cn=bill cook,cn=users,dc=storage,dc=dallas,dc=gov"
```

3. Visualize as configurações de **LDAPUSER** ou **LDAPPASSWORD**, emitindo o comando **QUERY STATUS**. Se uma senha não estiver definida, designe uma para o **LDAPUSER**, emitindo o comando **SET LDAPPASSWORD**.

Os caracteres que você pode utilizar para uma senha estão listados aqui:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

**Requisito:** Se você usar caracteres especiais ao emitir o comando **SET LDAPPASSWORD**, coloque-os entre aspas. Por exemplo:

```
set ldappassword "Pa$$=w0rd"
```

## O Servidor IBM Spectrum Protect não Aceita o LDAPPASSWORD

Se você receber um aviso de que o LDAPPASSWORD não é válido, o problema pode não ser com a senha.

Se você emitir um comando **SET LDAPPASSWORD** e receber mensagens de erro ANR3114E ou ANR3116E, o IBM Spectrum Protect pode não estar configurado corretamente. Examine as mensagens do servidor que ocorreram por volta do horário em que ANR3114E ou ANR3116E foram emitidas para determinar a causa dos erros. Um problema comum que você pode ver é que um valor incorreto é configurado para o comando **SET LDAPUSER**. O usuário deve ser inserido em formato de nome distinto (DN). Por exemplo:

```
ou=armonk,cn=tsmdata,uid=9A73819745
```

Se o valor não estiver de acordo com o DN, o **LDAPUSER** não será definido e não será possível configurar o LDAPPASSWORD. Um DN geralmente consiste em uma lista separada por vírgula de atributos de nomenclatura e pares de valores. A lista a seguir mostra os atributos de nomenclatura mais comumente usados:

- O nome comum (cn)
- O ID do usuário (uid)
- A unidade organizacional (ou)
- O componente de domínio (dc)
- A organização (o)
- O país (c)

Por exemplo:

```
cn=Jack Spratt,ou=marketing,dc=tucson,dc=storage,dc=com
uid=abbynornal,ou=sales,dc=tucson,dc=storage,dc=com
uid=cbukowski,ou=manufacturing,o=storage,c=us
```

## Resolvendo Problemas com o Servidor de Diretório LDAP

Se você tiver problemas com autenticação de senha, verifique se concluiu todas as etapas de configuração corretamente. Você definiu o nome distinto de base (DN Base) no servidor de diretório LDAP? Você configurou a opção **LDAPURL**?

Após instalar o servidor Tivoli Storage Manager V6.3.3 ou posterior, ou o servidor IBM Spectrum Protect V7.1.3 ou posterior, deve-se configurar o servidor de diretório LDAP para se comunicar com o servidor.

Se você tiver problemas de conexão, conclua as seguintes etapas com um utilitário LDAP como `ldapsearch` ou `ldp.exe`:

1. Teste a consulta de DNS de encaminhamento e reversa do sistema do servidor LDAP no sistema do servidor.
2. Teste a conexão de rede entre o sistema operacional do servidor e o sistema operacional do servidor de diretórios LDAP.
3. Conecte-se ao servidor de diretório LDAP com o nome do host e a porta que você especificou na opção **LDAPURL**.
4. Estabeleça uma conexão de Segurança da Camada de Transporte (TLS) emitindo a opção **StartTLS**.
5. Use autenticação simples de conexão para autenticação com os parâmetros que você definiu para o **LDAPUSER** e o **LDAPPASSWORD**.
6. Procure o servidor de diretório LDAP para o DN Base que você especificou na opção **LDAPURL**.

Um administrador do servidor LDAP pode usar o utilitário **ldapsearch**, como segue, para solucionar problemas de autenticação de diretório LDAP:

**Usando OpenLDAP (especifique o arquivo de certificado usando a opção **TLS\_CACERT** no arquivo **ldap.conf**)**

**Sem SSL/TLS**

```
ldapsearch -H <nome do host>  
-D <LDAPUSER> -W -s base -b  
<DN Base a partir de LDAPURL> -v -x objectclass="*"
```

**Com SSL/TLS**

```
ldapsearch -H <nome do host>  
-D <LDAPUSER> -W -s base -b  
<DN Base a partir de LDAPURL> -v -x -ZZ objectclass="*"
```

**Usando o cliente LDAP (instalado com o AIX ou transferido por download do [ibm.com](http://ibm.com))**

**Sem SSL/TLS**

```
ldapsearch -h <nome do host>  
-D <LDAPUSER> -w ? -s base -b  
<DN Base a partir de LDAPURL> -v objectclass="*"
```

**Com SSL/TLS**

```
ldapsearch -h <nome do host>  
-D <LDAPUSER> -w ? -s base -b  
<DN Base a partir de LDAPURL> -v -Y -x -K "cert.kdb" objectclass="*"
```

Para os comandos anteriores, os seguintes parâmetros se aplicam:

- *nome do host* = a URL a partir da opção **LDAPURL**, por exemplo  
`ldap://ldap.ibm.com:389/`
- *LDAPUSER* = os parâmetros a partir do comando **SET LDAPUSER**, por exemplo  
`cn=tsmsserver,cn=users,dc=ibm,dc=com`

- *DN Base a partir de LDAPURL* = o DN Base a partir da opção **LDAPURL**, por exemplo  
`"OU=tsm,DC=ibm,DC=com"`

## Resolvendo Problemas com o Nós e Administradores Bloqueados

As senhas que são autenticadas com o servidor de diretório LDAP podem ser bloqueadas se você ultrapassar o limite de senhas erradas ou por ações do administrador.

### Procedimento

Se você não puder desbloquear uma senha bloqueada, tente as seguintes etapas:

1. Retorne a senha para o servidor emitindo o seguinte comando de exemplo:  
`update node node_x new_pw authentication=local`
2. Limpe o servidor de diretório LDAP emitindo o seguinte comando de exemplo:  
`audit ldapdirectory fix=yes wait=no`  
 Esse comando remove nós ou IDs de administradores que estão armazenados no servidor de diretório LDAP que não autentica senhas com um servidor de diretório LDAP.
3. Efetue logout do nó.
4. Emita o seguinte comando:  
`update node node_x newest_pw authentication=ldap`
5. Efetue login no nó com a nova senha.

## Auditando o Servidor de Diretório LDAP para Limpar o Servidor

Manter o servidor de diretório LDAP em sincronização com o servidor torna mais fácil saber com o que você está trabalhando. Um servidor de diretório LDAP pode ter centenas de entradas que não são mais usadas. O servidor de diretório LDAP também pode carecer de determinadas entradas de administrador ou nó as quais se espera que estejam no servidor de diretório LDAP.

Uma auditoria pode relatar a você em que ID de administrador ou entradas nó é registrado como autenticar suas senhas com o servidor de diretório LDAP. É possível auditar o servidor de diretório LDAP para limpar senhas, administradores e nós não usados. O namespace controlado do IBM Spectrum Protect no servidor de diretório LDAP pode ficar fora de sincronização com o que o servidor IBM Spectrum Protect está armazenando.

Se o administrador para o servidor de diretório LDAP alterou entradas manualmente no diretório externo, essas entradas não ficariam em sincronização. O servidor IBM Spectrum Protect também pode ficar fora de sincronização com o servidor LDAP quando você usa o comando padrão **SYNCLDAPDELETE=NO** durante um comando **REMOVE**, **RENAME** ou **UPDATE**. O comando **AUDIT LDAPDIRECTORY** exclui qualquer entrada do servidor de diretório LDAP que não se correlaciona com o banco de dados do IBM Spectrum Protect. O comando também emite avisos para ajudá-lo a corrigir itens.

Avisos são emitidos se senhas que são autenticadas com o servidor de diretório LDAP forem armazenadas no banco de dados do IBM Spectrum Protect, mas não no namespace LDAP. A partir dos avisos, é possível usar o comando **UPDATE NODE** ou **UPDATE ADMIN** para corrigir o problema.



## Exemplo: Auditando o Servidor de Diretório LDAP

Se o namespace do IBM Spectrum Protect no servidor de diretório LDAP não estiver em sincronização com o banco de dados do IBM Spectrum Protect, emita o seguinte comando:

```
AUDIT LDAPDIRECTORY FIX=YES
```

O comando gera uma lista de todos os nós e administradores que são removidos do servidor de diretório LDAP. Também é gerada uma lista de todos os nós e administradores que estão ausentes no servidor de diretório LDAP. Se você deseja ver o que está fora de sincronização, use a configuração padrão **FIX=NO** para relatar as discrepâncias entre os servidores.

**Nota:** Não use a configuração **FIX=YES** se múltiplos servidores IBM Spectrum Protect compartilham namespace do diretório LDAP.

## Mensagens de Erro para Senhas Autenticadas por LDAP

Ao autenticar senhas com o servidor de diretórios LDAP, erros comuns podem ocorrer com a conexão entre o servidor e o servidor de diretórios LDAP.

Estas mensagens de erro são o resultado da comunicação com um servidor de diretório LDAP:

### ANR3114E

A mensagem ANR3114E é emitida sempre que é encontrado um erro inesperado durante uma operação LDAP. A mensagem fornece informações adicionais para ajudá-lo na resolução do erro. Por exemplo,

```
ANR3114E Erro de LDAP  
código de erro de LDAP (descrição do erro) ocorrido durante a operação.
```

#### Código de erro de LDAP

O número do erro retornado pela interface do cliente LDAP ou pelo servidor de Diretório LDAP.

#### descrição do erro

Uma descrição do *código de erro de LDAP*, indicando a causa do erro.

#### operação

A operação do cliente LDAP que estava em execução quando o erro ocorreu.

No exemplo a seguir, o código de erro 53 é retornado pela interface do cliente LDAP ou pelo servidor de diretório LDAP. A operação que estava em andamento no momento do erro também é sinalizada. Neste exemplo, `ldap_search_s`.

```
ANR3114E  
Erro de LDAP 53 (o DSA não pode executar) ocorrido durante ldap_search_s.
```

### ANR3115E

A mensagem ANR3115E é emitida quando há um erro com o servidor de diretório LDAP. Por exemplo,

```
ANR3115E O servidor de diretório LDAP retornou a seguinte mensagem de erro  
(mensagem do servidor LDAP) com o erro de LDAP.
```

## **mensagem do servidor LDAP**

Esse texto da mensagem é retornado pelo servidor de diretório LDAP e fornece informações adicionais sobre o erro que acabou de ocorrer.

### **ANR3116E**

A mensagem de erro ANR3116E é emitida quando o componente Global Security ToolKit (GSKit) encontra um erro durante uma operação LDAP. O GSKit fornece Secure Sockets Layer/Transport Layer Security (SSL/TLS) para operações LDAP. Esta mensagem de erro geralmente está relacionada ao SSL/TLS, certificados, criptografia ou operações de rede. Por exemplo:

ANR3116E Erro de LDAP SSL/TLS *código de erro do GSKIT*  
(*descrição do erro*) ocorrido durante a *operação*.

#### **código de erro do GSKit**

O número do erro que é retornado pelo componente GSKit.

#### **descrição do erro**

Uma descrição de texto que está associada ao *código de erro* que indica a causa do erro.

#### **operação**

A operação do cliente LDAP que estava em execução quando o erro ocorreu.

Se não for possível determinar a causa dos erros, execute as seguintes etapas:

1. Examine as mensagens do servidor que foram emitidas por volta do mesmo horário da mensagem de erro para determinar a causa e o impacto do erro. Emita o comando **QUERY ACTLOG** para visualizar o arquivo de log de atividades e procurar mensagens de erro.
2. Procure problemas de rede.
3. Verifique o status do servidor de diretório LDAP.
4. Para a mensagem de erro ANR3116E, procure problemas com os certificados que o servidor de diretório LDAP usa ou o banco de dados de chaves do servidor IBM Spectrum Protect (cert.kdb).
5. Examine os arquivos de log do servidor de diretórios LDAP.
6. Use utilitários LDAP, como "ldapsearch" ou "ldp" para isolar o problema.

A tabela a seguir contém erros que você pode localizar se a sua configuração não estiver correta:

*Tabela 1. Erros que Podem Ocorrer ao Autenticar Senhas com um Servidor de Diretório LDAP*

<b>Mensagens de erro</b>	<b>Resolução</b>
ANR3114E LDAP erro 118 (A biblioteca SSL não pode ser carregada)	O caminho da biblioteca pode não estar configurado adequadamente. Certifique-se de que esteja usando a versão correta do GSKit.
ANR3116E LDAP SSL/TLS erro 118 (Erro de SSL desconhecido)	
ANR3103E Ocorreu uma falha ao inicializar os serviços do diretório LDAP	

*Tabela 1. Erros que Podem Ocorrer ao Autenticar Senhas com um Servidor de Diretório LDAP (continuação)*

Mensagens de erro	Resolução
<p>ANR3114E LDAP erro 116 (Falha ao se conectar ao servidor SSL)</p> <p>ANR3116E LDAP SSL/TLS erro 406 (Erro de E/S)</p> <p>ANR3103E Ocorreu uma falha ao inicializar os serviços do diretório LDAP</p> <p>ANR2732E Não é possível se comunicar com o servidor de diretório LDAP</p>	<p>O nível do GSKit pode estar incorreto no Directory Server. Atualize o GSKit para o nível correto. Consulte nota técnica 1469388.</p> <p>Para o Active Directory, desative atualizações automáticas de certificados raiz com o Windows Update se uma conexão com a Internet não estiver disponível.</p>
<p>ANR3114E LDAP erro 52 (DSA está indisponível)</p> <p>ANR3103E Ocorreu uma falha ao inicializar os serviços do diretório LDAP</p> <p>ANR2732E Não é possível se comunicar com o servidor de diretório LDAP</p>	<p>O servidor Active Directory não tem um certificado disponível para TLS/SSL. Crie um certificado assinado que possa ser utilizado pelo Microsoft Active Directory.</p>
<p>ANR3114E LDAP erro 116 (Falha ao se conectar ao servidor SSL)</p> <p>ANR3116E LDAP SSL/TLS erro 414 (Certificado inválido)</p> <p>ANR3103E Ocorreu uma falha ao inicializar os serviços do diretório LDAP</p> <p>ANR2732E Não é possível se comunicar com o servidor de diretório LDAP</p>	<p>O certificado do servidor de diretório LDAP não é confiável. Inclua o certificado da autoridade de certificação (CA) raiz no Arquivo do banco de dados de chave do servidor IBM Spectrum Protect (cert.kdb) e verifique se os certificados não estão expirados.</p>
<p>ANR3094E O nome distinto (DN) que é especificado na opção <b>LDAPURL</b> não existe no servidor de diretório LDAP.</p> <p>ANR3103E Ocorreu uma falha ao inicializar os serviços do diretório LDAP</p>	<p>Se o DN existir, o <b>LDAPUSER</b> poderá não ter plenos direitos de controle de acesso para o DN Base que é especificado na opção <b>LDAPURL</b>.</p>
<p>ANR3114E LDAP erro 50 (Acesso insuficiente)</p> <p>ANR1885E Inicialização do serviço do diretório LDAP: Permissão foi negada quando a entrada do diretório LDAP foi acessada como LDAPUSER</p> <p>ANR3103E Ocorreu uma falha ao inicializar os serviços do diretório LDAP</p> <p>ANR1885E SET LDAPPASSWORD: Permissão foi negada quando a entrada <b>LDAPUSER</b> foi acessada</p>	<p>O <b>LDAPUSER</b> não tem plenos direitos de controle de acesso para o DN base especificado na opção <b>LDAPURL</b></p>

*Tabela 1. Erros que Podem Ocorrer ao Autenticar Senhas com um Servidor de Diretório LDAP (continuação)*

Mensagens de erro	Resolução
ANR3114E LDAP erro 116 (Falha ao se conectar ao servidor SSL)	Para o Directory Server, o SSL_TIMEOUT_MILLISEC não configurado alto o suficiente. Consulte nota técnica 1233758.
ANR3116E LDAP SSL/TLS erro 420 (Soquete fechado)	
ANR3114E LDAP erro 4 (Limite de tamanho excedido)	Aumente o limite de tamanho de procura do servidor LDAP para acomodar o número total de nós e administradores autenticados por LDAP.
ANR3114E Erro LDAP 91 (Erro de conexão) ocorrido durante ldap_sasl_bind.	O servidor LDAP não está ativo ou está offline.
ANR3103E Ocorreu uma falha ao inicializar os serviços de diretório LDAP.	

## Resolvendo Problemas de Planejamento de Cliente

O administrador do IBM Spectrum Protect pode planejar tarefas para que sejam executadas automaticamente.

Se você estiver tendo problemas com seu planejador de cliente, as seguintes etapas de diagnóstico estarão disponíveis para ajudá-lo a determinar a causa do problema:

- Inclusões e mudanças nas opções do cliente não são reconhecidas pelo planejador de cliente até o próximo início planejado. As exclusões feitas no conjunto de opções do cliente não terão efeito até a reinicialização do planejador.
- Inclusões, exclusões e mudanças feitas nos planejamentos gerenciados pelo responsável pela aceitação do cliente serão reconhecidas no próximo início planejado.
- Use a ferramenta de diagnóstico **SHOW PENDING** para mostrar planejamentos, nós e o próximo tempo de execução planejado.
- A partir do arquivo de opções do cliente, visualize a sub-rotina `dsm.sys` do nó e os valores das opções `MANAGEDSERVICES`, `PRESCHEDCMD` e `POSTSCHEDCMD` para obter informações depois que um nó perder um evento planejado.

## Determinando o Status de um Evento Planejado

O servidor mantém um registro de todos os eventos planejados. Os registros são úteis para o gerenciamento de planejamentos do IBM Spectrum Protect em vários computadores cliente.

### Sobre Esta Tarefa

Execute as seguintes etapas para visualizar os registros de eventos em um servidor:

### Procedimento

1. Emita o comando **QUERY EVENT**.
2. Emita a seguinte consulta para visualizar todos os resultados de eventos para o dia anterior:

```
query event * * begindate=today-1 begintime=00:00:00
enddate=today-1 endtime=23:59:59
```

3. Emita a seguinte consulta para limitar os resultados da consulta para casos de exceção:

```
query event * * begindate=today-1 begintime=00:00:00  
enddate=today-1 endtime=23:59:59 exceptionsonly=yes
```

## O que Fazer Depois

Os resultados da consulta incluem um campo de status que fornece um resumo do resultado para um evento específico. Usando a opção `format=detailed`, você também pode ver o resultado de um evento que é o código de retorno geral retornado pelo cliente. Consulte o comando **QUERY EVENT** para obter os eventos planejados e concluídos.

## Verificando Erros no Log de Atividades do Servidor

Se um evento planejado estiver ausente mas outros eventos planejados consecutivos para esse nó mostrarem um resultado Concluído, verifique os erros no log de atividades do servidor e no log de planejamento do cliente.

Ao verificar o log de atividades do servidor, limite os resultados de consulta para o prazo em torno do evento planejado. Inicie a consulta do log de eventos um pouco antes da janela de início do evento planejado em questão. Por exemplo, investigue o seguinte evento suspeito:

Início Planejado	Início Real	Nome do Plan.	Nome do Nó	Status
08/21/2003 08:27:33		HOURLY	NODEA	Missed

Posteriormente, é possível emitir uma das seguintes consultas:

```
query actlog begind=08/21/2003 begint=08:25:00  
query actlog begind=08/21/2003 begint=08:25:00 originator=client node=nodea
```

O cliente mantém um log detalhado de todas as atividades planejadas. Verifique no log de planejamento local do cliente se as consultas do log de atividades do servidor não podem explicar um evento planejado com falha.

Você deve ter acesso ao computador do cliente para inspecionar o arquivo de log de planejamento. O log de planejamento geralmente é salvo para o arquivo `dsmsched.log` e geralmente armazenado no mesmo diretório que o arquivo `dsmerror.log`. O local do arquivo de log pode ser especificado usando opções do cliente; portanto, você pode consultar o arquivo de opções para ver se a opção `SCHEDLOGNAME` foi usada para realocar o arquivo de opções. No Windows, o log de planejamento também pode ser realocado por uma configuração de opção que faz parte da definição de serviço de planejamento. É possível emitir o comando **DSMCUTIL QUERY** para verificar se essa opção foi configurada. Ao localizar o log de planejamento, procure no arquivo para localizar o período de tempo correspondente à data e hora de início do evento planejado em questão. A lista a seguir mostra os parâmetros de procura comuns:

- Se você investigar um evento perdido, verifique os detalhes do evento anterior, inclusive a hora em que esse evento foi concluído.
- Se estiver investigando um evento com falha, procure mensagens de erro que explicam a falha (como o limite de sessão do servidor sendo excedido).
- Quando uma explicação ainda não estiver clara, o último local a ser verificado será o arquivo do log de erros do cliente (geralmente denominado `dsmerror.log`).

## Iniciando e Parando o Serviço do Cliente

Iniciar e parar o serviço do cliente às vezes pode ajudar a resolver problemas de planejamento do cliente.

**Dica:** Ao gerenciar vários clientes que executam os processos do planejador, talvez você também queira conseguir iniciar e parar o serviço do cliente a partir de um computador remoto. O cliente para Windows fornece um utilitário para auxiliar no gerenciamento remoto do serviço do planejador. Para outros sistemas operacionais, os utilitários do sistema operacional padrão são necessários.

**Windows** Para gerenciar remotamente o serviço do planejador de cliente usando o comando **DSMCUTIL** com a opção **/computer:**, deve-se ter direitos administrativos no domínio do computador de destino. Para determinar se o serviço do planejador está em execução em um computador remoto, verifique o campo **Status Atual** em uma consulta semelhante à consulta a seguir:

```
dsmcutil query /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com
```

Emita as seguintes consultas para reiniciar um serviço do planejador que não contém planejamentos:

```
dsmcutil stop /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com  
dsmcutil start /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com
```

Portanto, se você usar o Client Acceptor Daemon (CAD) para gerenciar o planejador, poderá precisar reiniciar o serviço CAD ou parar o serviço do planejador e reiniciar o serviço CAD com as consultas a seguir:

```
dsmcutil query /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com  
dsmcutil query /name:"TSM Client Acceptor" /computer:ntserv1.ibm.com  
dsmcutil stop /name:"TSM Client Scheduler" /computer:ntserv1.ibm.com  
dsmcutil stop /name:"TSM Client Acceptor" /computer:ntserv1.ibm.com  
dsmcutil start /name:"TSM Client Acceptor" /computer:ntserv1.ibm.com
```

**AIX** **Linux** Se usar o método tradicional para gerenciar o planejador, será possível gravar um shell script para procurar e parar processos de planejadores ou de Client Acceptors do IBM Spectrum Protect em execução e, em seguida, reiniciar os processos. O seguinte shell script de exemplo mostra como reciclar o processo do planejador do IBM Spectrum Protect:

```
#!/bin/ksh  
# Use the following script to kill the currently running instance  
# of the TSM scheduler, and restart the scheduler in nohup mode.  
#  
# This script will not work properly if more than one scheduler  
# process is running.  
# If necessary, the following variables can be customized to allow an  
# alternate options file to be used.  
# export DSM_DIR=  
# export DSM_CONFIG=  
# export PATH=$PATH:$DSM_DIR  
# Extract the PID for the running TSM Scheduler  
PID=$(ps -ef | grep "dsmc sched" | grep -v "grep" | awk {'print $2'});  
print "Original TSM scheduler process using PID=$PID"  
# Kill the scheduler  
kill -9 $PID  
# Restart the scheduler with nohup, redirecting all output to NULL  
# Output will still be logged in the dsmsched.log  
nohup dsmc sched 2>&1 > /dev/null &  
# Extract the PID for the running TSM Scheduler  
PID=$(ps -ef | grep "dsmc sched" | grep -v "grep" | awk {'print $2'});  
print "New TSM scheduler process using PID=$PID"
```

**AIX** **Linux** **Mac OS X** Se desejar usar o método gerenciado CAD para gerenciar o planejador de cliente, configure a opção `managedservices` para **schedule** ou **schedule webclient** no arquivo `dsm.sys`. Para Mac OS X, se você não especificar a opção `managedservices`, o CAD gerenciará o planejador e o Web client, por padrão.

**AIX** Inclua a entrada a seguir no arquivo de inicialização do sistema (`/etc/inittab` para a maioria das plataformas):

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

**Linux** O programa de instalação do cliente de backup-archive cria um script de inicialização para CAD (**dsmcad**) no diretório `/etc/init.d`. É possível iniciar, parar, reiniciar e consultar o CAD, usando o comando **service** padrão no Linux. Por exemplo:

```
# service dsmcad start
# service dsmcad stop
# service dsmcad restart
# service dsmcad status
```

Para ativar o CAD para iniciar automaticamente após uma reinicialização do sistema, inclua o serviço da seguinte maneira, em um prompt de shell:

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

**Mac OS X** É possível iniciar ou parar o CAD com o utilitário **launchd**. Para iniciar o CAD, emita o comando a seguir na janela Terminal:

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

Para parar o CAD, emita o comando a seguir na janela Terminal:

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

Também é possível controlar o CAD com o aplicativo **Ferramentas TSM para Administradores**.

---

## Resolvendo Erros ao Incluir ou Excluir Arquivos de Cliente durante o Processo de Backup

A opção de processamento de inclusão/exclusão impacta os arquivos que são enviados para o servidor para uma operação de backup ou archive. Várias razões são possíveis quando você indica implícita ou explicitamente que um arquivo será incluído ou excluído durante o processamento de backup e ele não é processado corretamente.

### Identificando Arquivos que Foram Incluídos ou Excluídos pelo Conjunto de Opções do Cliente do Servidor

O administrador do IBM Spectrum Protect pode incluir ou excluir arquivos em nome do cliente. As instruções de inclusão ou exclusão fornecidas com o servidor substituirão as instruções de inclusão e exclusão inseridas no arquivo de opções do cliente local.

Entre em contato com o administrador do servidor IBM Spectrum Protect para corrigir o problema.

É possível emitir o comando **DSMC QUERY INCLEXCL** do cliente de backup-archive para identificar os arquivos que estão incluídos ou que foram excluídos do conjunto de opções do cliente de servidor. A saída deste comando mostra “Operating System” como o arquivo de origem para arquivos que foram automaticamente excluídos do processo de backup. Em nosso exemplo, os usuários indicam que desejam que todos os arquivos que terminam com uma extensão “.o” sejam incluídos no arquivo de opções local, mas o servidor envia ao cliente uma opção para excluir todos os arquivos que terminam com uma extensão “.o”. A opção fornecida pelo servidor prevalece.

```
tsm> q inclexcl
*** FILE INCLUDE/EXCLUDE ***
Mode Function Pattern (match from top down) Source File
-----
Excl All /.../*.o Server
Incl All /.../*.o dsm.sys
```

Opções que são transmitidas para o cliente do servidor são fornecidas em grupos, o que significa que se as opções INCLUDE e EXCLUDE são suportadas no servidor, que todas as opções INCLUDE seriam enviadas em um grupo e todas as opções EXCLUDE seriam enviadas em um grupo. Não é possível combinar essas opções para obter resultados desejados de inclusão de alguns arquivos de diretórios excluídos. Usar a opção INCLEXCL permite combinar e ordenar as opções INCLUDE e EXCLUDE.

## Excluindo Arquivos Automaticamente do Processo de Backup

O aplicativo de backup não efetua backup de arquivos específicos pois eles não são necessários para backup ou o IBM Spectrum Protect usará os arquivos para processamento interno.

Se determinados arquivos precisarem ser incluídos no processamento de backup, o IBM Spectrum Protect poderá incluí-los se você inserir instruções *INCLUDE* nas opções do cliente que são configuradas no servidor.

**Importante:** Como alguns arquivos foram explicitamente identificados como arquivos que não foram submetidos a backup, não inclua-os no conjunto de opções do cliente de servidor.

Emita o comando **DSMC QUERY INCLEXCL** do cliente de backup-archive para identificar os arquivos que não tiveram backup efetuado. A saída do comando **DSMC QUERY INCLEXCL** mostra “Operating System” como o arquivo de origem para os arquivos que foram automaticamente excluídos do processamento de backup.

**Windows** Por exemplo, a seguinte saída é exibida quando emitir o comando **DSMC QUERY INCLEXCL**:

```
tsm> q inclexcl
*** FILE INCLUDE/EXCLUDE ***
Mode Function Pattern (match from top down) Source File
-----
Excl All C:\WINDOWS\Registration\*.clb Operating System
Excl All C:\WINDOWS\netlogon.chg Operating System
```

Consulte a Tabela 2 na página 23 para os arquivos que foram automaticamente excluídos.



Tabela 2. Arquivos Automaticamente Excluídos Durante o Processo de Backup

Plataforma	Arquivos Excluídos
Windows	<ul style="list-style-type: none"> <li>Os arquivos são enumerados na chave de registro HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup</li> <li>O diretório temporário do cliente C:\ADSM.SYS</li> <li>Os metarquivos do Internet Information Server (IIS) (esses arquivos são processados no objeto do sistema ou backup de estado do sistema)</li> <li>Arquivos de registro (estes arquivos são processados no backup de objeto do sistema ou de estado do sistema)</li> <li>Arquivos de rastreo do cliente</li> <li>Arquivos de sistema</li> </ul> <p>Os arquivos de sistema Windows foram excluídos silenciosamente do processo de backup da unidade de sistema e não podem ser incluídos.</p> <p>Para processar estes arquivos de sistema Windows, você deve emitir um comando <b>DSMC BACKUP SYSTEMSTATE</b>.</p> <p>Os arquivos do sistema Windows são excluídos do processamento de backup da unidade de sistema porque são enviados durante backups de objeto do sistema ou de estado do sistema. Os arquivos de sistema são arquivos de inicialização, arquivos de catálogo, contadores de desempenho e arquivos protegidos pela system file protection (sfp) do Windows. Esses arquivos não são processados durante o backup da unidade de sistema. No entanto, os arquivos são excluídos internamente do processamento de unidade do sistema em vez de contarem com instruções de exclusão explícitas devido ao número total de instruções de exclusão que seriam necessárias para representar todos esses arquivos. O desempenho do backup pode ser afetado negativamente.</p> <p>É possível emitir o comando do cliente de backup-archive <b>DSMC QUERY SYSTEMINFO</b> para identificar os arquivos do sistema Windows. A saída deste comando é gravada no arquivo dsminfo.txt.</p> <pre>(conteúdo parcial do arquivo dsmfinfo.txt) ===== SFP c:\windows\system32\ahui.exe (protected) c:\windows\system32\apphelp.dll (protected) c:\windows\apppatch\apphelp.sdb (protected) c:\windows\system32\asycfilt.dll (protected)</pre>
AIX Linux	Arquivo de rastreo do cliente
Mac OS X	<ul style="list-style-type: none"> <li>Arquivos voláteis, temporário e de dispositivo que são usados pelo sistema operacional</li> <li>Arquivos de rastreo do cliente</li> </ul>

## Excluindo Arquivos com a Instrução EXCLUDE.DIR

A instrução EXCLUDE.DIR exclui todos os diretórios e arquivos no diretório-pai.

Se você quiser incluir todos os arquivos que correspondem a um padrão de arquivo, independentemente de seus locais em uma estrutura de diretórios, não use as instruções EXCLUDE.DIR.

Por exemplo, considere este conjunto de instruções de inclusão/exclusão:

AIX

Linux

Mac OS X

```
exclude.dir /usr
include /.../*.o
```

Windows

```
exclude.dir C:\Users
include C:\.../*.o
```

A instrução INCLUDE neste exemplo indica que todos os arquivos com uma extensão .o são incluídos, mas a instrução EXCLUDE.DIR anterior exclui todos os arquivos no diretório /usr ou C:\Users, mesmo se tiverem uma extensão .o. Este fato seria verdadeiro, independentemente da ordem das duas instruções.

Se você deseja fazer backup de todos os arquivos que terminam com .o, use a sintaxe a seguir:

AIX

Linux

Mac OS X

```
exclude /usr/.../*
include /.../*.o
```

Windows

```
exclude C:\Users\.../*
include C:\.../*.o
```

Ao usar os curingas nas instruções include-exclude, use \* se deseja incluir ou excluir todos os arquivos, em vez do padrão \*.\*.\*.\* O padrão \*.\*.\*.\* significa para incluir ou excluir todos os arquivos que contêm pelo menos um caractere de ponto (.), enquanto \* significa para incluir ou excluir todos os arquivos. Se você usar \*.\* , os arquivos que não contêm caracteres de ponto (como C:\MYDIR\MYFILE no Windows) não serão filtrados.

Se desejar executar um backup seletivo ou um backup incremental parcial de um único arquivo no cliente da linha de comando, isso não será afetado pela opção EXCLUDE.DIR.

Se usar o cliente da linha de comandos para iniciar um backup seletivo ou um backup incremental parcial de um único arquivo, o arquivo será processado, mesmo se houver uma instrução EXCLUDE.DIR que exclui um de seus diretórios-pai no caminho de arquivo.

Por exemplo, considere a seguinte instrução de inclusão e exclusão usada nas ações da linha de comandos subsequentes:

AIX

Linux

Mac OS X

```
exclude.dir /home/spike
```

Windows

```
exclude.dir C:\Users\spike
```

O seguinte backup seletivo sempre resulta no arquivo sendo processado: AIX

Linux

Mac OS X

```
dsmc selective /home/spike/my.file
```

Windows

```
dsmc selective C:\Users\spike\my.file
```

Se for emitido um comando de backup seletivo que contenha um curinga, nenhum arquivo será processado porque o diretório foi excluído: AIX Linux

Mac OS X

```
dsmc selective "/home/spike/my.*"
```

Windows

```
dsmc selective "C:\Users\spike\my.*"
```

**Importante:** Um backup incremental subsequente do sistema de arquivos /home renderiza o arquivo /home/spike/my.file inativo. Da mesma forma, no Windows, um backup incremental subsequente do diretório C:\Users renderiza o arquivo C:\Users\spike\my.file inativo.

Não termine as instruções EXCLUDE.DIR com um delimitador de diretório.

Os seguintes exemplos mostram instruções EXCLUDE.DIR incorretas, devido a um delimitador de diretório no fim do caminho do diretório: AIX Linux

```
exclude.dir /usr/
```

Mac OS X

```
exclude.dir /Users/
```

Windows

```
exclude.dir c:\directory\
```

Os exemplos a seguir mostram a codificação correta de EXCLUDE.DIR: AIX

Linux

```
exclude.dir /usr
```

Mac OS X

```
exclude.dir /Users
```

Windows

```
exclude.dir c:\directory
```

## Determinando se as Instruções de Compactação, Criptografia ou de Backup de Subarquivo São de Inclusão ou de Exclusão

As instruções de inclusão e exclusão para compactação (INCLUDE.COMPRESS), criptografia (INCLUDE.ENCRYPT) e backup de subarquivo (INCLUDE.SUBFILE) não indicam que o arquivo está incluído para processo de backup.

É possível usar as instruções INCLUDE e EXCLUDE em combinação com as instruções COMPRESS, ENCRYPT e SUBFILE para produzir resultados desejados.

Considere o seguinte exemplo:

AIX

Linux

Mac OS X

```
exclude /usr/file.o
include.compress /usr/*.o
```

Windows

```
exclude c:\Users\file.o
include.compress c:\Users\*.o
```

Esta instrução indica que o arquivo /usr/file.o foi excluído do processamento de backup. A instrução INCLUDE.COMPRESS indica que “se um arquivo for um candidato para processo de backup e corresponder ao padrão /usr/\*.o, compacte o arquivo.” Não interprete a instrução INCLUDE.COMPRESS como “fazer backup de todos os arquivos que correspondem ao padrão /usr/\*.o e compactá-los.” Se deseja fazer backup para o arquivo /usr/file.o neste exemplo, você deve remover a instrução de exclusão.

## Usando Delimitadores para Incluir ou Excluir Arquivos

Quando os delimitadores de volumes ou diretórios não estão corretos, as instruções INCLUDE e EXCLUDE podem ter mau funcionamento.

Uma instrução INCLUDE ou EXCLUDE específica de plataforma contém sintaxe para “tudo” e “todos os arquivos em um diretório específico”.

Se desejar usar uma instrução INCLUDE para “todos os arquivos em um diretório específico”, certifique-se de que as barras e os delimitadores de volume estejam corretos. Se você deseja incluir todos os arquivos em um diretório denominado “home”, consulte os exemplos a seguir:

Windows

**Usando a barra invertida “\” e o delimitador de volume “:”**

```
*include everything in the c:\home directory
include c:\home\...\*
*include everything
include *:\...\*
```

AIX

Linux

Mac OS X

**Usando a barra “/”**

```
*include everything in the /home directory
include /home/...\*
*include everything
include /...\*
```

## Resolvendo Problemas Devido à Codificação Incorreta da Lista de Inclusão ou Exclusão

Devido à complexidade ou número de instruções INCLUDE ou EXCLUDE, pode ocorrer a inclusão ou exclusão não intencional de um arquivo.

Configure o cliente com o sinalizador de rastreo **INCLEXCL** para ajudar a determinar por que um arquivo foi incluído ou excluído.

Por exemplo, quando você acha que o arquivo `c:\home\file.txt` deve ser incluído no processo de backup. O rastreo mostra que há uma instrução EXCLUDE que exclui este arquivo:

```
polbind.cpp (1026): File 'C:\home\file.txt' explicitly excluded by pattern  
'Excl All c:\home\*.txt'
```

Usar o comando **DSMC QUERY INCLEXCL** do cliente de backup-archive mostra que esta instrução está no conjunto de opções do servidor IBM Spectrum Protect:

```
tsm> q inclexcl  
*** FILE INCLUDE/EXCLUDE ***  
Mode Function Pattern (match from top down) Source File  
-----  
Excl All c:\home\*.txt Server
```

---

## Resolvendo Problemas de Diferença de Captura Instantânea

AIX

Linux

Windows

Você pode executar backups incrementais mais rápidos de volumes do arquivador N-Series e NetApp caso use a interface de programação de aplicativo (API) de Diferença de Captura Instantânea do NetApp.

### Pré-requisitos

Para usar o recurso Diferença de captura instantânea, primeiro é necessário configurar um ID de usuário e senha NetApp no cliente. O ID do usuário e a senha são necessários para que o IBM Spectrum Protect se conecte ao arquivador. Configure um ID de usuário/senha com autoridade de administrador no AIX e Linux, ou um com autoridade administrativa no Windows. Configure o nível de autoridade igual ao usado ao mapear ou montar o volume do arquivador. Assegure-se de usar o nome completo do host ou o formato de endereço IP pontuado para o nome do arquivador. Emita o comando **SET PASSWORD** do cliente de backup-archive para salvar estas informações de ID de usuário/senha.

**Lembre-se:** O comando **DSMC SET PASSWORD** é estendido para salvar as senhas de tipo “filer”.

O recurso de Diferença de Captura Instantânea compara duas capturas instantâneas (base e diferencial) e retorna uma lista de arquivos que foram modificados, excluídos ou incluídos entre as duas. O IBM Spectrum Protect faz backup dessa lista de arquivos em vez de varrer o sistema de arquivos em busca de alterações.

O recurso de Diferença de Captura Instantânea suporta os seguintes recursos, que são aplicáveis apenas ao nível de volume:

- Arquivadores NetApp/N-Series executando o Data ONTAP release 7.3 ou posterior

- **Windows** Volumes conectados ao sistema de arquivos de internet comuns (CIFS)
- Volumes do arquivador tradicional e FlexVol
- GUI Java e Web client
- **AIX** **Linux** Volumes conectados ao sistema de arquivos de rede (NFS)

O recurso de Diferença de Captura Instantânea não suporta os seguintes recursos:

- Volumes NetApp/N-Series conectados à SAN
- QTrees ou subdiretórios
- Os volumes Vfiler com um arquivador que está executando o ONTAP V8.1.0 ou mais antigo não são suportados. Os volumes Vfiler com um arquivador que esteja executando ONTAP V8.1.1 ou mais recente são suportados.

**Windows**

## Verificando o Tipo de Volume do Arquivador

O IBM Spectrum Protect espera que o tipo de segurança Common Internet Files System (CIFS) anexado seja New Technology File System (NTFS). Use o NetApp FilerView e certifique-se de que o tipo de segurança CIFS esteja configurado como "ntfs."

## Restrições de Diferença de Captura Instantânea

A falta do suporte Unicode de NetApp impede que IBM Spectrum Protect processe qualquer arquivo que use caracteres que não estejam no intervalo ASCII de 7 bits. O IBM Spectrum Protect pode fazer backup apenas de nomes que contenham caracteres ASCII. Dois comportamentos de diferença de captura instantânea foram observados durante testes com caracteres Unicode:

1. O comando incremental de Diferença de Captura Instantânea termina com o código de retorno 13001. Esse código de retorno ocorre com os intervalos 'specials' e 'surrogate' de Unicode para volumes do arquivador de Diferença de Captura Instantânea que são criados com o sinalizador UTF8. Esse erro de Diferença de Captura Instantânea ocorre com mais frequência sem o sinalizador UTF8. O IBM Spectrum Protect termina com a mensagem de erro ANS5283E "A operação não foi bem-sucedida." Nenhum arquivo tem seu backup feito.
2. A interface de programação de aplicativos (API) da diferença de captura instantânea não falha, mas retorna caracteres que não fazem parte do nome real. O IBM Spectrum Protect inspeciona a sequência para ver se qualquer caractere está fora do intervalo ASCII de 7 bits. Se estiver, o IBM Spectrum Protect ignora o arquivo e registra o erro para o arquivo dsmerror.log.

Seguem as situações em que os arquivos e os diretórios podem ser submetidos a backup e nenhum erro é relatado:

- Você exclui um arquivo incluindo uma regra de exclusão no arquivo de inclusão/exclusão. O IBM Spectrum Protect faz um backup da captura instantânea atual com essa regra de exclusão em vigor. Você não alterou o arquivo, mas remove a regra que o excluiu. Um comando de backup incremental auxiliado por captura instantânea com a opção snapdiff não detecta essa mudança de inclusão/exclusão porque detecta apenas mudanças de arquivo entre duas capturas instantâneas. Os próprios arquivos precisam ser alterados para que a API de Diferença de Captura Instantânea detecte a alteração e o IBM Spectrum Protect faça backup do arquivo.
- Você incluiu uma instrução include no arquivo de opções. Esta instrução include tem efeito apenas se o arquivo for detectado por ter sido alterado pela API de

Diferença de Captura Instantânea. Talvez não seja feito backup dos arquivos, visto que o IBM Spectrum Protect não está inspecionando cada arquivo no volume durante a operação de backup.

- Você exclui explicitamente um arquivo do inventário do IBM Spectrum Protect emitindo o comando **DSMC DELETE BACKUP**. A API de diferença de captura instantânea não detecta que um arquivo foi manualmente excluído de IBM Spectrum Protect por você. Portanto, o arquivo permanece desprotegido no armazenamento. O arquivo estará desprotegido até que ele seja alterado no volume e a mudança seja detectada pela API de diferença de captura instantânea. Depois que a mudança é detectada, a API de Diferença de Captura Instantânea sinaliza o IBM Spectrum Protect para fazer backup do arquivo novamente.
- Mudanças de política como a alteração de Mode=modified para mode=absolute não são detectadas. Todo o espaço no arquivo é excluído do inventário. As políticas não detectadas fazem com que o IBM Spectrum Protect crie uma captura instantânea a ser usada como origem (base) e um backup incremental completo é feito.

A execução de um backup incremental completo sem a opção snapdiff resolve essas limitações. O IBM Spectrum Protect não controla o que constitui um objeto alterado. A alteração de objetos agora é controlada pela API de Diferença de Captura Instantânea. Portanto, a execução de um backup incremental completo sem a opção SNAPDIFF assegura a detecção de todas as alterações em arquivos.

É possível usar os sinalizadores de rastreo a seguir para processamento de Diferença de Captura Instantânea:

- enter
- exit
- general
- snapshot
- hci
- hci\_detail
- diskmap
- diskmap\_detail
- hdw
- hdw\_detail
- bacache
- snapdiffdb

AIX

Linux

Configure um ID de usuário e senha para root no arquivador myFiler.ibm.com.

```
dsmc set password -type=filer myFiler.ibm.com root
```

Digite a senha para o ID do usuário "root@myFiler.ibm.com": \*\*\*\*\*  
Redigite a senha para verificação:\*\*\*\*\*  
ANS0302I Concluído com êxito.

AIX

Linux

Configure um ID de usuário e senha para root no arquivador myFiler.ibm.com.

```
dsmc set password -type=filer myFiler.ibm.com root secret
```

## Resolvendo Problemas no Diretório de Captura Instantânea para Volumes do Sistema de Arquivos NetApp ou N-Series

Quando é feito backup de um volume mapeado do Network File System (NFS) ou do Common Internet File System (CIFS), todas as capturas instantâneas no diretório snapshot também o são. Esse backup inclui capturas instantâneas não desejadas que podem ocupar um espaço valioso. Os volumes montados por NFS ou mapeados por CIFS pode ser NetApp ou N-Series.

Para evitar o backup de capturas instantâneas não desejadas, use o método de backup do Protocolo de Gerenciamento de Dados de Rede (NDMP). Você também pode fazer backup de seus dados com a opção `SNAPSHOTROOT` do cliente ou executar um backup incremental com o comando **INCREMENTAL** e a opção `SNAPDIFF`. Como alternativa, exclua o diretório snapshot de qualquer backup.

**Importante:** Linux Se você executar um backup completo de NetApp SnapDiff e, em seguida, usar o método NFS4 para montar o volume NetApp no servidor, ocorrerá outro backup completo de NFS. Para evitar um backup completo, use o sinalizador de teste **SNAPDIFFINCR** não documentado para forçar o processamento incremental em entradas que já foram processadas. Por exemplo, `-test=snappeddiffincr`.

## Resolvendo Problemas de Login ao Usar o Sistema de Arquivos com Criptografia nos Sistemas Operacionais AIX

AIX

Durante o processamento de login, o keystore do Sistema de Arquivos com Criptografia (EFS) é aberto automaticamente quando a senha do keystore corresponde à senha de login do usuário.

Quando a senha de login do AIX for diferente da senha do keystore de EFS, você deverá abrir o keystore manualmente antes de iniciar o cliente. Abra o keystore emitindo o seguinte comando:

```
efskeymgr -o <cmd>
```

Inicie o cliente de uma das seguintes maneiras:

- Inicie o cliente da linha de comandos emitindo o comando `efskeymgr -o ./dsmc`.
- Inicie o cliente da GUI Java emitindo o comando `efskeymgr -o ./dsmj`.

Se você estiver usando a interface gráfica com o usuário (GUI), deverá sincronizar as senhas. Para sincronizar a senha de usuário com a senha do keystore do EFS, emita o seguinte comando:

```
efskeymgr -n
```



## Resolvendo Erros de Backup de Imagem

AIX

Linux

Erros de backup de imagem podem ocorrer com imagens do Linux, imagens de captura instantânea do Linux ou durante o backup de imagem e backup-archive baseados na captura instantânea do AIX JFS2.

### Resolvendo Erros de Backup de Imagem do Linux

Linux

É possível resolver erros de backup de imagem do Linux executando etapas específicas, dependendo do tipo de erro que ocorre.

#### Sobre Esta Tarefa

O seguinte erro foi gerado durante o backup de imagem:

```
paris:#dsmc b image /dev/system/lv01
Função de Imagem de Backup Invocada.
ANS1228E Falha no envio do objeto '/dev/system/lv01'
ANS1584E Erro ao carregar biblioteca do sistema 'libdevmapper.so'
necessária para operações de imagem para volumes LVM2.
ANS1813E Processo de Backup de Imagem de '/dev/system/lv01'
concluído com falhas.
Número total de objetos inspecionados: 1
Número total de objetos de backup: 0
Número total de objetos atualizados: 0
Número total de objetos ligados novamente: 0
Número total de objetos excluídos: 0
Número total de objetos expirados: 0
Número total de objetos com falha: 1
Total number of bytes transferred: 0 B
Tempo de transferência de dados: 0.00 s
Taxa de transferência de dados na rede: 0.00 KB/s
Aggregate data transfer rate: 0.00 KB/sec
Objetos compactados a: 0%
Tempo de processamento decorrido: 00:00:29
paris# cat dsmerror.log
11/15/2006 13:07:53 ANS1228E Falha no envio
de objeto '/dev/system/lv01'
11/15/2006 13:07:56 ANS1584E Erro ao carregar biblioteca do
sistema 'libdevmapper.so' necessária para
operações de imagem para volumes LVM2.
11/15/2006 13:07:56 ANS1813E Processo de Backup de Imagem
de '/dev/system/lv01' concluído
com falhas.
```

Para este erro, certifique-se de que o sistema tenha a versão correta do mapeador de dispositivo de biblioteca instalado. Execute as seguintes etapas para determinar a versão instalada:

#### Procedimento

1. Emita o comando **# DMSETUP VERSION**. A saída é semelhante à seguinte:

```
Versão da biblioteca: 1.00.09-ioctl (2004-03-31)
Versão do driver: 4.4.0
```

ou

Emita o seguinte comando para determinar a versão usando o rpm:

```
# rpm -q -a |grep device-mapper
```

A saída é semelhante à seguinte:

```
device-mapper-1.00.09-17.5
```

A versão da biblioteca deve ser a Versão 1.01 ou posterior.

## 2. Verifique a instalação após o upgrade.

```
# rpm -Uvh device-mapper-1.01.01-1.6.i586.rpm
Preparando... ##### [100%]
1:device-mapper ##### [100%]
# rpm -q -a |grep device-mapper
device-mapper-1.01.01-1.6
```

Também é possível verificar o diretório /lib para ver se as versões corretas estão instaladas. Um sistema com os níveis corretos deve ter as seguintes informações:

```
# ls -l /lib/libdev*
lrwxrwxrwx 1 root root 20 Jul 5 11:42 /lib/libdevmapper.so
->libdevmapper.so.1.01
-rwxr-xr-x 1 root root 24490 May 23 2005 /lib/libdevmapper.so.1.00
-rwxr-xr-x 1 root root 28216 May 23 2005 /lib/libdevmapper.so.1.01
```

## Resolvendo Falhas de Backup Ao Usar o Backup de Imagem de Captura Instantânea Linux

Linux

Para resolver um backup de imagem de captura instantânea do Linux que falhou, confirme se o sistema está configurado para criar uma captura instantânea.

### Antes de Iniciar

Tente criar uma captura instantânea em um prompt de shell emitindo o seguinte comando:

```
/sbin/lvcreate -L 16384K -n <snapname eg. tsmsnap>-s
<volume devname eg /dev/system/lv01>
```

Se você receber o erro Captura instantânea: Destino(s) do mapeador de dispositivos necessário(s) não detectado(s) no kernel, o módulo de kernel **:dm\_snapshot** não será carregado. Esse comando também pode falhar por outras razões, o que pode resultar no comportamento semelhante do IBM Spectrum Protect.

### Sobre Esta Tarefa

O exemplo a seguir mostra a saída gerada quando um backup de imagem falha com a mensagem de erro ANS1258E, “Falha na operação de captura instantânea”.

```
dsmerror.log :
05/31/2006 15:14:36 ANS1259E Falha na operação de captura instantânea da imagem.
Texto de diagnóstico: tsmStartSnapshot.
05/31/2006 15:14:38 ANS1259E Falha na operação de captura instantânea da imagem.
Texto de diagnóstico: tsmTerminateSnapshot.
05/31/2006 15:14:38 ANS1228E Falha no envio do objeto '/fs1'
05/31/2006 15:14:38 ANS1258E A operação de captura instantânea da imagem falhou.
```

### Procedimento

Conclua as etapas a seguir para carregar os módulos:

1. Verifique se o módulo não está carregado. Consulte o seguinte comando de exemplo:  

```
# lsmod |grep dm_
dm_mod 112104 6
```
2. Carregue o módulo. Consulte o seguinte comando de exemplo:  

```
# modprobe dm_snapshot
```
3. Verifique se a etapa anterior foi bem-sucedida. Consulte o seguinte comando de exemplo:  

```
# lsmod |grep dm_
dm_snapshot 44024 0
dm_mod 112104 6 dm_snapshot
#
```
4. Crie uma captura instantânea no prompt de shell. Consulte o seguinte comando de exemplo:  

```
# /sbin/lvcreate -L 16384K -n tsmsnap -s /dev/system/lv01
Volume lógico "tsmsnap" criado
```
5. Remova a captura instantânea que foi criada na etapa anterior. Consulte o seguinte comando de exemplo:  

```
# lvremove /dev/system/tsmsnap
Você realmente deseja remover o volume lógico ativo "tsmsnap"? [y/n]: y
Volume lógico "tsmsnap" removido com êxito
#
```

## Resultados

Se você seguiu todas as etapas, agora poderá executar os backups de imagens da captura instantânea.

**Restrição:** Se o comando **lvcreate** falhar com o erro “Extensões livres insuficientes (0) no grupo de volumes...”, isso indicará que não há espaço suficiente no grupo de volumes para um volume de captura instantânea.

## Resolvendo Erros durante o Backup-archive e Backup de Imagem Baseados em Captura Instantânea de JFS2 do AIX

### AIX

Durante o término do IBM Spectrum Protect, o cliente exclui a captura instantânea do sistema de arquivos registrados (JFS2) aprimorado do AIX que é criado durante o processo de backup. No entanto, existem situações nas quais o AIX pode não atender à solicitação de exclusão de captura instantânea feita pelo IBM Spectrum Protect.

### Antes de Iniciar

As seguintes situações ilustram onde uma solicitação de exclusão de captura instantânea pode falhar:

- O pressionamento da tecla **Control-C** é emitido durante um processo de backup de captura instantânea do IBM Spectrum Protect. O pedido de desmontagem de captura instantânea JFS2 pode falhar com um erro “Dispositivo Ocupado”, porque o processo do IBM Spectrum Protect está no meio do acesso à captura instantânea.
- Duas solicitações de backup de captura instantânea IBM Spectrum Protect são iniciadas simultaneamente para o mesmo sistema de arquivos. Por exemplo, se o pedido de backup `dsmc backup image /fs1` for submetido a partir de um

console, e ao mesmo tempo, um pedido de backup `dsmc backup image /fs1` for emitido a partir de outro console. Se o processo do primeiro console criar a primeira captura instantânea para `/fs1` e o segundo processo do segundo console criar a segunda captura instantânea para `/fs1` e se o segundo processo for concluído primeiro e tentar excluir a captura instantânea, o AIX falhará na solicitação de exclusão.

- Duas solicitações de backup de captura instantânea IBM Spectrum Protect são iniciadas simultaneamente para dois pontos de montagem virtuais cujo sistema de arquivos de origem é o mesmo. Por exemplo, emitindo `dsmc incr /fs1/level1/dir1` a partir de um console e `dsmc incr /fs1/level2/level3/dir3` a partir de um segundo console, simultaneamente.

## Sobre Esta Tarefa

O AIX espera que as solicitações de exclusão de captura instantânea sejam emitidas em uma determinada ordem, com a exclusão da captura instantânea mais antiga solicitada primeiro e a exclusão da próxima captura instantânea mais antiga solicitada depois e assim por diante. Se IBM Spectrum Protect não puder aceitar a sequências devido a processos simultâneos que criam capturas instantânea para o mesmo sistema de arquivos, o AIX falha nas solicitações de exclusão. Nos exemplos anteriores, o IBM Spectrum Protect registra uma mensagem de aviso solicitando que o usuário exclua a captura instantânea manualmente.

## Procedimento

Para excluir manualmente uma captura instantânea, emita os comandos a seguir na ordem especificada:

1. `snapshot -q -c ' ' <SRCFS>`
2. `df -k`
3. `unmount -f /tsm*`
4. `rmdir /tsm*`
5. `snapshot -d /dev/tsm*`

Se o processo de exclusão de captura instantânea falhar com a mensagem de erro “Dispositivo Ocupado” ou com alguma outra mensagem de erro, emita o comando `unmount -f <srcfs>` para desmontar o sistema de arquivos de origem. Em seguida, tente excluir a captura instantânea novamente.

6. `ls -l /dev/tsm*`

Se algum volume lógico `/DEV/TSM*` permanecer, emita o comando `rmlv -f tsm*`.

7. Se você tiver um sistema de arquivos de origem desmontado, emita o comando `mount <srcfs>` para montá-lo.

## Resultados

Se alguma captura instantânea não for excluída durante um processo anterior do IBM Spectrum Protect, o IBM Spectrum Protect tentará excluir as capturas instantâneas durante a próxima chamada, porque, como as capturas instantâneas mais antigas permanecem, o AIX falha nas solicitações de exclusão para capturas instantâneas mais recentes para um determinado sistema de arquivos. Os seguintes casos indicam onde o IBM Spectrum Protect não tenta excluir capturas instantâneas mais antigas:

- Se a captura instantânea não foi criada pelo IBM Spectrum Protect, em seguida, o IBM Spectrum Protect nomeará suas capturas instantâneas com um prefixo

“tsm” para distingui-las de outras capturas instantâneas que são criadas para o mesmo sistema de arquivos. Se a captura instantânea não foi criada pelo IBM Spectrum Protect, uma mensagem de erro será gerada solicitando que o usuário exclua a captura instantânea mais antiga e a operação novamente.

- Se a captura instantânea foi criada pelo IBM Spectrum Protect mas ainda estiver montada, isto indica que a captura instantânea está sendo usada por algum outro processo do IBM Spectrum Protect.
- Se a captura instantânea foi criada pelo IBM Spectrum Protect, não for montada, mas recém-criada, a captura instantânea pode ter sido criada por algum outro processo IBM Spectrum Protect.

Em todos estes casos, pode ser necessário executar uma exclusão manual. Se existir alguma captura instantânea mais antiga não usada, os backups subsequentes do IBM Spectrum Protect falharão ao excluir capturas instantâneas.

**Importante:** Existem correções de defeito do AIX relacionadas a capturas instantâneas JFS2 no AIX 6.1 ou mais recente. Se as correções não forem aplicadas, poderá ocorrer um encerramento do sistema AIX ou o IBM Spectrum Protect pode parar durante a exclusão da captura instantânea e de outros processos de consulta da captura instantânea. Isso também pode causar distorção dos dados durante o backup da imagem de bloqueio usada. Portanto, o IBM Spectrum Protect não executará as seguintes tarefas:

- Monitoramento de captura instantânea
- Exclusão de captura instantânea

Para usar esses recursos, assegure-se de que o nível do sistema operacional esteja em AIX 6.1 ou mais recente.

---

## Soluções de Suporte para a API do IBM Spectrum Protect

Recursos estão disponíveis para aprender sobre a interface de programação de aplicativos (API) do IBM Spectrum Protect ou para diagnosticá-la.

A instrumentação da API só será ativada se a API testflag **INSTRUMENT**: estiver definida no arquivo de configuração e as chamadas **dsmSetUp** e **dsmCleanUp** forem usadas no aplicativo.

Consulte *Usando a Interface de Programação de Aplicativo* ou IBM Support Assistant para obter mais informações.

## Reunindo Informações da API antes de Entrar em Contato com o Suporte IBM

É possível ajudar significativamente a determinar um problema na interface de programação de aplicativos (API) reunindo informações sobre seu ambiente.

Reúna a quantidade máxima possível das seguintes informações antes de entrar em contato com o Suporte IBM:

- Em qual sistema operacional o problema está ocorrendo?
- Qual é o nível exato do sistema operacional, incluindo todos os service packs e hot fixes que foram aplicados?
- Qual é o nível exato da API do IBM Spectrum Protect?
- Qual é o nível exato do servidor IBM Spectrum Protect?

- Qual é a plataforma do servidor e o nível de sistema operacional do IBM Spectrum Protect?
- Qual é o nível exato do agente de armazenamento do IBM Spectrum Protect (se for um ambiente sem a LAN)?
- Quando é a plataforma do agente de armazenamento e o nível de sistema operacional do IBM Spectrum Protect (se for um ambiente sem a LAN)?
- Quais aplicativos estão executando no sistema?
- Quais etapas são necessárias para recriar o problema? Se você não puder recriar o problema, quais etapas o causaram?

## Coletando arquivos de API antes de chamar o suporte do IBM

Arquivos de log e outros dados importantes são criados pela interface de programação de aplicativos (API) do IBM Spectrum Protect.

Reúna o máximo dos seguintes arquivos antes de entrar em contato com o Suporte IBM:

- O arquivo do log de erros da API do IBM Spectrum Protect. O arquivo de log de erros da API padrão é `dsierror.log`.
- Os arquivos de rastreo criados para a API. Os sinalizadores de rastreo comuns são `api`, `api_detail` ou `verbdetail`.
- A saída de qualquer comando ou operação com falha pode ser a saída de console que é redirecionada para um arquivo ou uma imagem de tela real da falha.
- A saída do comando **QUERY SYSTEM** do servidor.
- O arquivo de log de atividade do servidor. O administrador do IBM Spectrum Protect pode visualizar esse arquivo de log para você, se não possuir um ID de usuário e senha de administrador do IBM Spectrum Protect.
- Se o cliente da API estiver configurado para movimentação de dados sem LAN, colete o arquivo de opções para o agente de armazenamento do IBM Spectrum Protect. O nome padrão para o arquivo de opções é `dsmsta.opt`.
- Um programa ou seções breves do código de origem do aplicativo que estão chamando as chamadas de função da API do IBM Spectrum Protect e são suspeitas de causar problemas.
- O arquivo de opções da API do IBM Spectrum Protect.

Os dois arquivos de opções a seguir são usados nos sistemas operacionais Linux e UNIX:

### **dsm.opt**

O arquivo de opções do cliente

### **dsm.sys**

O arquivo de opções do sistema

Para Windows, localize o arquivo de opções padrão `dsm.opt` ou o arquivo referenciado pela variável de ambiente **DSMI\_CONFIG**. Para Linux e UNIX, o arquivo de opções padrão é `dsm.sys` e está localizado no diretório referenciado pela variável de ambiente **DSMI\_DIR**.

Em outros sistemas operacionais, o arquivo de opções do cliente `dsm.opt` contém todas as opções. As seguintes definições são variáveis de ambiente que descrevem o local dos arquivos de opções e outros componentes da API:

### **DSMI\_CONFIG**

O nome completo do arquivo de opções do cliente.

## DSMI\_DIR

A variável *DSMI\_DIR* aponta para o diretório de instalação de API e também é usada para localizar o arquivo *dsm.sys* no Linux e UNIX. Sempre que *DSMI\_DIR* for configurado, assegure-se de que exista um arquivo *dsm.sys* no mesmo diretório.

## DSMI\_LOG

A variável *DSMI\_LOG* aponta para o caminho do arquivo *dsierror.log*. Se a opção *errorlogname* do cliente for configurada, o local especificado por essa opção substituirá o diretório especificado por *DSMI\_LOG*.

**Dica:** Se a variável *DSMI\_LOG* apontar para um diretório para o qual o usuário não tem permissão de gravação, **dsmSetup** e **dsmInitEx** falharão com o código de retorno *DSM\_RC\_ACCESS\_DENIED* (106).

Se a opção *errorlogname* for configurada no arquivo de opções *dsm.sys/dsm.opt*, seu valor será usado como o nome do log de erro em vez do valor padrão *dsierror.log*.

## Verificando se a API Usa o Arquivo de Opções Correto

AIX

Linux

Mac OS X

Quando você reúne arquivos da interface de programação de aplicativos (API), deve verificar se a API usa o arquivo de opções correto ou a sub-rotina do servidor no arquivo *dsm.sys*.

### Procedimento

Conclua as etapas a seguir para verificar se a API usa o arquivo de opções correto ou a sub-rotina do servidor:

1. Insira uma opção ou valor incorreto no arquivo de opções do cliente ou na sub-rotina do servidor no *dsm.sys*. Por exemplo, caso não tenha certeza de que a API use o servidor *srvr1.cmpron*, insira a instrução 'ERRONEOUS\_OPTION 12345' na sub-rotina do servidor *srvr1.cmpron* do arquivo *dsm.sys*. Consulte o seguinte exemplo:

```
...
SERVERNAME srvr1.cmproff
COMPRESSION NO
TCPSERVERADDRESS computer.company.com

SERVERNAME srvr1.cmpron
COMPRESSION YES
ERRONEOUS_OPTION 12345
TCPSERVERADDRESS computer.company.com

SERVERNAME srvr1.pwdf1
PASSWORDACCESS GENERATE
PASSWORDDIR .
TCPSERVERADDRESS computer.company.com
...
```

2. Verifique se a API detecta o erro. É possível usar o programa da API de amostra, *dapi.smp*, com esse propósito.

```
# dapismp
...
Inserir seleção ==>0
Nome do nó: node1
Nome do proprietário:
Senha:
Arquivo de configuração da API:
Opções da sessão:
Nome do Usuário:
Senha do usuário:
As respostas acima estão corretas (y/n/q)?
Estabelecendo conexão para o nó node1, proprietário, com senha
*** Falha inicialização: ANS0220E (RC400) Opção inválida localizada durante
análise da opção.
```

Se nenhum erro for relatado, o arquivo de opções incorreto terá sido atualizado.

3. Verifique os valores da variável de ambiente mencionados em “Coletando arquivos de API antes de chamar o suporte do IBM” na página 36 ou repita as etapas 1 e 2 com um arquivo de opções ou uma sub-rotina do servidor diferente.
4. Remova a opção inserida na etapa 1.

## Determinando se os dados são enviados para o agente de armazenamento, em vez de para o servidor

Você deve saber se seus dados estão sendo enviados para o agente de armazenamento do IBM Spectrum Protect, em vez de um servidor. Se eles estiverem sendo enviados para o agente de armazenamento, não será possível recuperá-los.

### Procedimento

Conclua as etapas a seguir para verificar se os dados estão sendo enviados para o agente de armazenamento IBM Spectrum Protect, em vez de para o servidor:

1. Inclua as opções de rastreo a seguir para o arquivo de opções do cliente antes de fazer backup ou arquivar os objetos:

- TRACEFILE <nome do arquivo de rastreo>
- TRACEFLAGS api api\_detail verbdetail

2. Examine o arquivo de rastreo após a operação e localize uma instrução que seja semelhante à seguinte:

```
dsmSendObj ENTRY:... objNameP: '<the file name>'
```

Esta instrução é seguida pela seguinte instrução de rastreo:

```
tsmEndSendObjEx: Total de bytes enviados * *, encryptType e *** encryptAlg é
*** compress é *, totalCompress é * * totalLFBytesSent * *
```

A instrução de rastreo indica se o objeto **totalLFBytesSent** foi enviado para o agente de armazenamento IBM Spectrum Protect. Se **totalLFBytesSent** for 0 0, os dados foram enviados diretamente para o servidor IBM Spectrum Protect.

Como alternativa, seu próprio aplicativo pode determinar se os dados foram enviados através de um caminho sem LAN, usando a chamada de função **dsmEndSendObjEx** e a estrutura de dados **dsmEndSendObjExOut\_t**.

```
/*-----+
| Definição de tipo para dsmEndSendObjExOut_t
+-----*/
typedef struct dsmEndSendObjExOut_t
```



```

{
dsUInt16_t      stVersion;      /* versão da estrutura */
dsStruct64_t    totalBytesSent; /* total de bytes lidos do apl. */
dsmBool_t       objCompressed; /* foi compactado por objeto */
dsStruct64_t    totalCompressSize; /* tamanho total após compactação */
dsStruct64_t    totalLFBytesSent; /* total de bytes enviados sem a LAN */
dsUInt8_t       encryptionType; /* tipo de criptografia utilizado */
} dsmEndSendObjExOut_t;
totalLFBytesSent - 0 total de bytes sem a LAN que foram enviados.

```

Por exemplo:

```

...
rc = dsmEndSendObjEx(&endSendObjExIn, &endSendObjExOut);
if (rc)
{
    printf("*** dsmEndSendObjEx failed: ");
    rcApiOut(dsmHandle, rc);
}
else
{
    di64toCh(&endSendObjExOut.totalLFBytesSent,t,10);
    format_number(t,t2);
    printf("LAN-free bytes sent: %s\n", t2);
}

```

## O que Fazer Depois

Consulte *Chamadas de Função API em Usando a Interface de Programação de Aplicativos* para obter mais detalhes.

---

## Executando aplicativos que usam a API como ID do usuário não raiz

AIX

Linux

Mac OS X

Deve-se executar etapas específicas se você tiver efetuado login como um ID do usuário não raiz que está tentando executar um aplicativo que usa a interface de programação de aplicativo (API).

### Procedimento

Conclua as etapas a seguir para permitir que um ID do usuário não raiz acesse a API:

1. Configure a variável de ambiente **DSMI\_CONFIG**. Verifique se o ID do usuário não raiz tem permissão de leitura para o arquivo de opções do cliente especificado por **DSMI\_CONFIG**. Caso contrário, **dsmInit/dsmInitEx** falhará com o código de retorno **DSM\_RC\_NO\_OPT\_FILE** (406). Por exemplo, o arquivo de opções a seguir não é legível por um ID do usuário não raiz, portanto, as permissões do arquivo deverão ser atualizadas:

```

$ ls -l $DSMI_CONFIG
-rwx----- 1 root sys 86 Out 7 13:07 /testfsapi/callmt_nr/dsm.opt
$ su root
Senha:
# chmod a+r /testfsapi/callmt_nr/dsm.opt
# exit
$ ls -l $DSMI_CONFIG
-rwxr--r-- 1 root sys 86 Oct 7 13:07 /testfsapi/callmt_nr/dsm.opt

```

2. Configure a variável de ambiente **DSMI\_DIR** para o diretório de instalação da API. Verifique se o ID do usuário não raiz possui permissão de leitura para o arquivo de opções do sistema especificado por **\$DSMI\_DIR/dsm.sys**.

```
$ export DSMI_DIR=/opt/tivoli/tsm/client/api/bin64
$ ls -l $DSMI_DIR/dsm.sys
-rw-r--r-- 1 root sys
4712 Oct 19 18:07 /opt/tivoli/tsm/client/api/bin64/dsm.sys
```

3. Configure a variável de ambiente **DSMI\_LOG**. Verifique se o ID do usuário não raiz tem permissão de gravação para esse diretório. Por exemplo, o diretório DSMI\_LOG é de propriedade de um ID do usuário não raiz:

```
$ ls -ld $DSMI_LOG
drwxr-xr-x 2 apitest users 96 Oct 19 17:56 /testfsapi/callmt_nr/logs
```

Se **PASSWORDACCESS GENERATE** estiver configurado no arquivo de opções do sistema dsm.sys, execute as etapas 4 e 5; caso contrário, vá para a etapa 6.

4. Opcional: Verifique a propriedade e permissões do Trusted Communication Agent (TCA) apenas se a opção PASSWORDDIR não for usada ou apontar para um diretório ao qual o usuário não tenha acesso de leitura/gravação. Esse arquivo está no diretório indicado pela variável de ambiente **DSMI\_DIR**. Por exemplo, o seguinte TCA possui a propriedade e permissões corretas:

```
$ ls -l $DSMI_DIR/dsmtca
-rwsr-xr-x 1 root bin 5021160 Out 14 09:48
/opt/tivoli/tsm/client/api/bin64/dsmtca
```

Permissões ou propriedades incorretas resultam em DSM\_RC\_AUTH\_FAILURE (137) retornado de dsmInit. Além disso, é mandatório usar a mesma versão da biblioteca da API e dsmtca. Versões combinadas resultam em erros.

```
Erro : o programa de chamada e dsmtca não são compatíveis
data comp do prgr chamada: Seg Out 18 21:15:59 2004 Seg Out 18 21:15:59 2004
Data comp TCA : Qua Out 13 16:48:03 2004 Qua Out 13 16:48:03 2004
*** Falha inicializ.: ANS0282E (RC168) Arq de senhas não disponível.
```

5. O usuário root ou autorizado deve gerar o arquivo de senha TSM.PWD usando o cliente de backup-archive ou o aplicativo da API de amostra **dapismp**. Um usuário autorizado é qualquer ID do usuário não raiz que possua acesso de leitura e gravação na senha armazenada (arquivo TSM.PWD). O local do arquivo de senha é determinado pela opção PASSWORDDIR no arquivo de opções do sistema dsm.sys. No exemplo a seguir, o aplicativo da API de amostra gera o arquivo de senha TSM.PWD para um nó cuja senha é *oddesy*:

```
# dapismp
*****
* Bem-vindo ao aplicativo de amostra para a API do IBM Spectrum Protect. *
* Biblioteca da API Versão = 5.4.0.0 *
*****
Escolha uma das seguintes ações para testar:
0. Conexão
1. Backup
2. Restauração
3. Archive
4. Recuperar
5. Consultas
6. Alterar Senha
7. Utilitários: Deletes, Updates, Logevent, SetAccess, RetentionEvent
8. Configurar preferências, envSetUp
9. Sair do sistema
10. Restaurar/Recuperar sem Prompt de Deslocamento
11. Conexão Estendida
Inserir seleção ==>0
Nome do nó:
Nome do proprietário:
Senha:oddesy
Arquivo de configuração da API:
Opções da sessão:
Nome do Usuário:
Senha do usuário:
As respostas acima estão corretas (y/n/q)?
Estabelecendo conexão para o nó, proprietário, com senha oddesy
Identificador no retorno = 1
Escolha uma das seguintes ações para testar:
0. Conexão
1. Backup
2. Restauração
3. Archive
4. Recuperar
5. Consultas
6. Alterar Senha
7. Utilitários: Deletes, Updates, Logevent, SetAccess, RetentionEvent
8. Configurar preferências, envSetUp
9. Sair do sistema
10. Restaurar/Recuperar sem Prompt de Deslocamento
11. Conexão Estendida
Inserir seleção ==>9
# ls -l TSM.PWD
-rw----- 1 root sys 121 Out 19 18:28 TSM.PWD
A chamada de função dsmInit retorna DSM_RC_NO_PASS_FILE (168), se o arquivo de
senha não estiver presente no diretório especificado pela opção PASSWORDDIR.
```

6. Se o recurso de rastreamento estiver ativado, verifique se o ID do usuário não raiz possui permissão de gravação para o arquivo que é indicado ao emitir a opção TRACEFILE.

## Determinação de Problemas do Journal Based Backup

### Windows

O Journal Based Backup (JBB) é adequado para o backup de sistemas de arquivos com quantidades pequenas ou moderadas de atividades de mudança entre ciclos de backup.

# Determinando se um Backup Será Baseado em Diário

## Windows

Antes de implementar um backup, é necessário determinar se ele será baseado em diário.

### Sobre Esta Tarefa

Execute as seguintes etapas para assegurar que o backup seja baseado em diário:

### Procedimento

1. Configure o daemon de diário para registrar o sistema de arquivos que está tendo backup efetuado. O daemon de diário registra um sistema de arquivos depois que o sistema de arquivos é listado no arquivo de configuração tsmjbbd.ini. Consulte as seguintes informações de configuração:  

```
[JournaledFileSystemSettings]
;
; Liste de sistema de arquivos registrados
JournaledFileSystems=c:
```
2. Execute um backup incremental completo no sistema de arquivos correspondente enquanto o sistema de arquivos está ativamente sendo registrado. Este backup incremental completo deve configurar data do “Último Backup Concluído” no espaço no arquivo do servidor IBM Spectrum Protect para que o diário seja configurado como válido. É possível visualizar a data do “Último Backup Concluído” emitindo o comando do servidor **QUERY FILESPACE**. Depois que o diário for configurado para o estado válido, backups subsequentes pelo mesmo nó para o mesmo servidor serão baseados no diário. Se um backup usar um nó diferente ou um servidor diferente, o backup não será baseado em diário, mas o diário permanecerá válido para o nó e servidor originais e os backups no nó e servidor originais serão baseados em diário.  
A mensagem a seguir é um exemplo do que é gravado no Log de Eventos de Aplicativo do Windows quando um diário é inicialmente configurado como válido:  
Diário configurado como válido para fs 'H:' e será usado para backup pelo nó GSHLAGER3 no servidor GSHLAGER2\_SERVER1.
3. Certifique-se de que o nó e o servidor IBM Spectrum Protect que o backup está usando correspondam ao nó e servidor para o qual o diário é válido.
4. Use o utilitário de Visualização do Banco de Dados do Diário para determinar o estado atual de um diário. Se um diário válido for reiniciado, os backups não serão baseados em diário até que o diário seja revalidado.  
A mensagem a seguir é gravada no Log de Eventos de Aplicativo do Windows quando um diário é reiniciado:  
O banco de dados do diário 'c:\tsmjourn\tsmH\_\_.jdb' para fs 'H:' foi excluído e reconfigurado para o estado inválido.

## Reiniciando um Diário Válido

AIX

Linux

Windows

Você pode aumentar o desempenho reiniciando um diário válido.

As razões para reiniciar um diário válido:

- Condições de erro no daemon do diário
  - Erros no estouro do Buffer causados por atividade de mudança excessiva no sistema de arquivos do diário que está sendo monitorado para mudanças
  - Erros de acesso do banco de dados do diário (erros de disco cheio, etc.)
- Pedido por um cliente de backup
- Os clientes emitirão um pedido de reinício do diário quando for determinado que um sistema de arquivos do diário não possui integridade por uma das seguintes razões:
  - O espaço no arquivo do servidor não existe mais
  - O espaço no arquivo do servidor foi excluído depois do último backup
  - O conjunto de política do nó foi atualizado após o último backup
  - As datas de Último Backup Concluído ou Último Backup Iniciado não são válidas (não configuradas)

## Executando o Daemon de Diário em Primeiro Plano

Windows

É possível melhorar os recursos de diagnóstico e sua capacidade de teste executando o daemon de diário no primeiro plano, em vez de executar como um serviço do Windows.

Inicie o daemon de diário de um prompt de comandos do Windows, como a seguir: `tsmjbdd.exe i`

## O utilitário Journal Database Viewing

Windows

O utilitário Journal Database Viewing fornece informações importantes para ajudar na determinação de problema de backups baseados em diário.

O utilitário de Visualização do Banco de Dados do Diário fornece as seguintes informações:

- O estado atual do diário
- O sistema de arquivos que é controlado pelo diário
- O registro de data e hora de ativação do diário
- O registro de data e hora de validação do diário
- O tamanho máximo suportado do diário
- O nó e servidor para os quais o diário é válido
- O número de entradas contidas no diário

**Nota:** Para clientes de backup-archive que são mais antigos que a Versão 6.3.1, não é possível visualizar o conteúdo de diários abertos com o utilitário de visualização. Um diário aberto é um diário que é aberto por outro processo, como o daemon de diário. É possível, no entanto, visualizar o conteúdo de um registro de controle do

diário aberto. O utilitário de visualização está disponível com a V6.3.1 e clientes de backup-archive mais novos. Para obter mais informações sobre o utilitário de visualização, consulte a seguinte nota técnica: Executar o utilitário dbviewb.exe no modo em lote.

Este utilitário também permite a procura, inserção ou exclusão de entradas específicas em um banco de dados do diário.

A sintaxe deste utilitário é a seguinte:

```
dbviewb <nome completo do arquivo base do banco de dados do diário>
dbviewb <nome completo do arquivo base do banco de dados do diário> <i>
D:\tsm540c\debug\bin\winnt_unicode>dbviewb c:\tsmjournal\tsmh__.jdb
IBM Spectrum Protect
Utilitário de Visualização do Banco de Dados do Diário
Versão 5, Release 4, Nível 0.0
Última Atualização: Nov 28 2006
Consultando o BD do Diário ...
Informações do Banco de Dados do Diário:
Arquivo de Banco de Dados c:\tsmjournal\tsmh__.jdb
Tamanho do Disco do Arquivo de Banco de Dados 81 KB (83754 Bytes)
Sistema de Arquivos do Diário H:
Data de Ativação do Diário Ter Nov 28 11:49:05 2006
Data de Validação do Diário Qua Nov 29 16:41:11 2006
Tamanho Máximo do Diário 8191 PB (9223372036854775807 Bytes)
Diário de Mudança de Tipo de Diário
Estado do Diário Válido
Válido para o Servidor GSHLAGER2_SERVER1
Válido para o Nó GSHLAGER3
Número de Entradas do BD 22
D:\tsm540c\debug\bin\winnt_unicode>
D:\tsm540c\debug\bin\winnt_unicode>dbviewb c:\tsmjournal\tsmh__.jdb i
IBM Spectrum Protect
Utilitário de Visualização do Banco de Dados do Diário
Versão 5, Release 4, Nível 0.0
Última Atualização: Nov 28 2006
Consultando o BD do Diário ...
Informações do Banco de Dados do Diário:
Arquivo de Banco de Dados c:\tsmjournal\tsmh__.jdb
Tamanho do Disco do Arquivo de Banco de Dados 81 KB (83754 Bytes)
Sistema de Arquivos do Diário H:
Data de Ativação do Diário Ter Nov 28 11:49:05 2006
Data de Validação do Diário Qua Nov 29 16:41:11 2006
Tamanho Máximo do Diário 8191 PB (9223372036854775807 Bytes)
Diário de Mudança de Tipo de Diário
Estado do Diário Válido
Válido para o Servidor GSHLAGER2_SERVER1
Válido para o Nó GSHLAGER3
Número de Entradas do BD 22
Insira o pedido em uma única linha, no seguinte formato:
Req-Type [Chave de Entrada]
Req-type pode ser um dos seguintes:
Del Exclui uma linha do banco de dados. O nome completo do arquivo com
distinção entre maiúsculas e minúsculas é necessário.
Find Localiza a entrada cuja chave é o argumento.
List Imprime todas as entradas em stdout. Nenhum argumento é necessário.
Quit
Insira seu pedido: find H:\dbview.example\Dir3Depth1\F2.txt
Registro de Banco de Dados do Diário Localizado:
-----
Nome do Objeto: H:\dbview.example\Dir3Depth1\F2.txt
Ação : Modificar
Tipo do Objeto: Arquivo
Inserido: Sex Dez 01 10:15:28 2006
```

Horário do Objeto: Sex Dez 01 14:15:28 2006  
Contagem de Ocorrências : -2110169276  
-----  
Insira seu pedido: quit

---

## Usando o Windows Volume Shadow Copy Services

### Windows

O cliente IBM Spectrum Protect Windows usa o Volume Shadow Copy Services (VSS) para concluir o estado do sistema e o backup de serviços do sistema. O VSS também pode ser usado como um provedor de captura instantânea para Suporte de Arquivo Aberto (OFS) e operações de imagem on-line.

## Definindo Erros Temporários do VSS

### Windows

O cliente considera que diversos erros dos Serviços de Cópia de Sombra de Volume (VSS) sejam temporários. Erros temporários são erros da rede ou unidades que apresentam um comportamento anormal temporário que pode exigir a recuperação do backup.

Quando ocorrer um destes erros, por padrão, o cliente tentará novamente o processo de backup do VSS por três vezes em intervalos de 30 segundos. O número de novas tentativas e os intervalos de novas tentativas podem ser configurados usando dois sinalizadores de teste (**TESTFLAG SETVSSMAXRETRY** e **TESTFLAG SETVSSDELAY**). O cliente considera que os seguintes erros VSS sejam temporários:

**VSS\_E\_MAXIMUM\_NUMBER\_OF\_VOLUMES\_REACHED**  
**VSS\_E\_SNAPSHOT\_SET\_IN\_PROGRES**  
**VSS\_E\_MAXIMUM\_NUMBER\_OF\_SNAPSHOTS\_REACHED**  
**VSS\_E\_PROVIDER\_VETO VSS\_E\_UNEXPECTED**  
**VSS\_E\_FLUSH\_WRITES\_TIMEOUT**  
**VSS\_E\_HOLD\_WRITES\_TIMEOUT**  
**VSS\_E\_WRITERERROR\_TIMEOUT**  
**VSS\_E\_WRITERERROR\_RETRYABLE**  
**VSS\_E\_WRITERERROR\_OUTOFRESOURCES**  
**VSS\_E\_WRITER\_NOT\_RESPONDING**  
**VSS\_E\_VOLUME\_IN\_USE**  
**VSS\_E\_PROVIDER\_IN\_USE**  
**VSS\_E\_UNEXPECTED\_PROVIDER\_ERROR**  
**VSS\_E\_UNEXPECTED\_WRITER\_ERROR**

## Definindo Sinalizadores de Teste de VSS do Windows

### Windows

O cliente usa dois sinalizadores de teste diferentes para configurar o número de novas tentativas do Serviço de Cópia de Sombra de Volume (VSS) e o tempo entre as novas tentativas.

Os sinalizadores de teste a seguir são usados para configurar a nova tentativa e o intervalo de novas tentativas do IBM Spectrum Protect:

#### SETVSSMAXRETRY

Especifica o número de vezes que o processo de backup de VSS é tentado novamente se ocorrer um erro temporário. O valor-padrão é tentar novamente três vezes.

#### SETVSSDELAY

Especifica o número de segundos a aguardar entre novas tentativas do processo de backup de VSS, caso ocorra um erro temporário. O valor-padrão é de 60 segundos.

Exemplo de arquivo de opções:

```
tentar novamente 10 vezes em intervalos de 300 segundos
TESTFLAG SETVSSMAXRETRY:10
TESTFLAG SETVSSDELAY:300
```

## Ajuste de Volume Shadow Copy Services

### Windows

Várias correções no ajuste do Serviço de Cópia de Sombra de Volume (VSS) da Microsoft estarão disponíveis se você estiver tendo dificuldades com o ajuste de VSS.

### Controlando o Tamanho da Área diff do VSS

Depois de aplicar estas correções, ocorrerá um dos seguintes eventos:

- “A cópia do volume C: demorou muito para ser instalada”
- “A cópia de sombra do volume C: parou porque o arquivo de área de diferença não pôde aumentar no período.”

Reduza o carregamento de E/S desse sistema para evitar esses problemas. Se os eventos ainda ocorrerem, use a seguinte chave de registro para controlar o tamanho da área de diferença usada pelo VSS:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VolSnap\
MinDiffAreaFileSize : REG_DWORD: <tamanho em MB> (o tamanho padrão é 300,
mas pode ser aumentado para 3000).
```

### Tamanho Máximo do Log de Eventos

A Microsoft indica que, se os logs de eventos forem suficientemente grandes, a operação de cópia pode levar mais tempo do que o tempo limite para sistemas com um alto carregamento de E/S ou um alto carregamento de memória. O tamanho do log é melhor quando inferior a 64 MB.



## Reunindo Informações de Diagnóstico do VSS para a Assistência Microsoft

### Windows

As informações de diagnóstico da IBM sobre falhas no Serviço de Cópia de Sombra de Volume (VSS) podem não ter o que você precisa. É possível localizar informações de diagnóstico sobre falhas do VSS no site de suporte da Microsoft.

Se a falha do VSS estiver fora do escopo do IBM Spectrum Protect, reúna as seguintes informações para o suporte Microsoft:

- Log de eventos do aplicativo do Windows
- Log de eventos do sistema Windows
- Rastreamento de VSS

Examine os arquivos de log do aplicativo e sistema, com foco nos eventos de erro criados pelas origens VolSnap e VSS no momento da falha. É possível extrair os eventos relevantes do log para isolar o problema e ter uma interação mais produtiva com o suporte da Microsoft.

## Resolvendo Erros Usando um Rastreamento do VSS

### Windows

É possível resolver erros do Volume Shadow Copy Services (VSS) conduzindo um rastreamento do VSS.

### Sobre Esta Tarefa

Execute as seguintes etapas para concluir um rastreamento VSS:

### Procedimento

1. Crie um arquivo `tracing.reg` e altere a entrada `TraceFile` para apontar para um volume que não terá uma cópia de sombra criada. Use o conteúdo na parte inferior desse arquivo para criar o arquivo. Observe o uso do delimitador de barra invertida dupla; você deve inserir “\\” como o delimitador de cada barra invertida no caminho que deseja especificar.
2. Clique duas vezes no arquivo no Windows Explorer para instalar o `tracing.reg`.
3. Reproduza o problema.
4. Desative o rastreamento excluindo a chave "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing".

### Resultados

O conteúdo a seguir é exibido no arquivo de rastreamento `tracefile.reg`:

```
Windows Registry Editor Versão 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing]
"TraceFile"="c:\\trace.txt"
"TraceLevel"=dword:ffffffff
"TraceEnterExit"=dword:00000001
"TraceToFile"=dword:00000001
"TraceToDebugger"=dword:00000000
"TraceFileLineInfo"=dword:00000001
"TraceForceFlush"=dword:00000000
```

## Executando Chamadas da API do VSS com o Programa de Amostra vsreq.exe

Windows

O Software Developers Kit (SDK) dos Serviços de Cópia de Sombra de Volume (VSS) contém o programa de amostra **vsreq** (solicitante de VSS). O programa do solicitante de VSS executa uma sequência de chamadas de API VSS, como as chamadas que são executadas pelo cliente de backup-archive.

É possível compilar e executar **vsreq.exe** no sistema com falha para determinar se **vsreq** e IBM Spectrum Protect encontram o mesmo problema. Se **vsreq** puder reproduzir o mesmo problema que IBM Spectrum Protect, então a saída de **vsreq** pode ser fornecida ao suporte Microsoft para ajudar no diagnóstico do problema VSS.

Em alguns casos, a Microsoft fornece uma ferramenta de análise de subsistema de entrada/saída (E/S) (“yapt”) para reunir dados de desempenho de E/S para análise. **vshadow** é uma ferramenta que também está disponível como uma alternativa para **vsreq**.

## Comparando a Interação do IBM Spectrum Protect e do Ntbackup.exe com o VSS

Windows

O uso do arquivo executável **Ntbackup.exe** não utiliza totalmente o Volume Shadow Copy Services (VSS) e nem sempre pode ser considerado uma avaliação de desempenho para a interação do IBM Spectrum Protect com o VSS.

A diferença conhecida entre **Ntbackup.exe** e o IBM Spectrum Protect no contexto do VSS é que o **Ntbackup.exe** não usa o VSS para fazer backup do Active Directory (NTDS). Embora o **Ntbackup.exe** use o VSS para efetuar uma captura instantânea, ele ainda usa a API de NTDS legada para ler dados a partir do disco. O IBM Spectrum Protect usa a interface do VSS para ler dados do NTDS a partir do disco. Se existir um problema com o gravador de VSS responsável pelo NTDS, ele não será revelado com **Ntbackup.exe**.

Emita o comando **VSSADMIN LIST** para consultar o estado do gravador VSS para assegurar que o VSS esteja em um estado estável ou pronto.

---

## Comandos SHOW para o Cliente de Backup-Archive

Comandos **SHOW** são comandos de diagnóstico não suportados que são usados para exibir informações sobre estruturas de controle de memória e outros atributos de tempo de execução. Os comandos **SHOW** são usados pelo desenvolvimento e serviço apenas como ferramentas de diagnóstico. Existem vários comandos **SHOW** para o cliente de backup-archive.

Dependendo das informações exibidas por um comando **SHOW**, poderá haver instâncias em que as informações estão sendo mudadas, ou casos em que elas podem fazer com que o aplicativo (cliente, servidor ou agente de armazenamento) pare a execução. Os comandos **SHOW** devem ser usados apenas quando o desenvolvimento ou serviço sugerir. Os comandos **SHOW** na tabela Tabela 3 na página 49 não são todos os comandos **SHOW** disponíveis.

Tabela 3. Comandos *SHOW* para o Cliente de Backup-archive

Comando <b>SHOW</b>	Descrição	Informações
CLUSTER	Exibe informações sobre os mapeamentos de disco em um Cluster Microsoft.	Útil para exibir informações sobre o mapeamento de disco (configuração) em um ambiente de Cluster Microsoft.
DOMAIN	Exibe informações sobre os domínios configurados a serem usados para processo de backup incremental.	Útil para exibir informações e resumir as opções do cliente DOMAIN, DOMAIN.IMAGE e DOMAIN.NAS.
OPTIONS	Exibe as opções do cliente.	Útil para determinar as configurações de opções do cliente.
OPTTABLE	Exibe informações sobre opções que são administradas pelo servidor versus as que são gerenciadas pelo arquivo de opções do cliente.	O cliente pode receber suas configurações de opções do arquivo de opções do cliente ou do servidor. Para receber a opção do servidor, um conjunto de opções do cliente deve ser definido com o comando <b>DEFINECLOPTSET</b> . Este comando ajuda a determinar se o cliente está usando uma opção configurada do arquivo de opções ou uma opção configurada de um conjunto de opções do cliente definido no servidor.
PLUGINS	Exibe informações sobre plug-ins instalados para este cliente.	O cliente usa plug-ins para fornecer recursos extra, tais como backup de imagem. Este comando <b>SHOW</b> exibe os plug-ins que estão instalados para este cliente e também atributos dos vários plug-ins, como sua versão, tipo e local.
SESSION	Exibe os recursos que este cliente pode ter para esta conexão com o servidor.	O cliente e o servidor relatam e negociam os recursos que cada um possui quando uma sessão é iniciada entre um cliente e um servidor. Este comando <b>SHOW</b> relata os recursos disponíveis por este servidor e cliente.
SYSTEMSTATE	Para clientes Windows, exibe os dados <b>SYSTEM STATE</b> disponíveis neste cliente.	O comando <b>SYSTEMSTATE SHOW</b> é útil na determinação de quais arquivos <b>SYSTEM STATE</b> estão instalados neste sistema Windows e de quais arquivos pode ser feito backup.
TRACEFLAGS	Exibe informações sobre classes de rastreo e classes de rastreo agregadas para este cliente.	O comando <b>TRACEFLAGS SHOW</b> é útil na determinação de quais classes de rastreo e classes de rastreo agregadas podem ser usadas para este cliente.

Tabela 3. Comandos *SHOW* para o Cliente de Backup-archive (continuação)

Comando SHOW	Descrição	Informações
VERSION	Exibe a versão e data de compilação para este cliente.	O comando <b>VERSION SHOW</b> é útil ao determinar qual cliente está em execução e quando ele foi construído.

## Resolvendo problemas para recuperação de bancos de dados Microsoft SQL individuais a partir de um backup de máquina virtual

### Windows

É possível usar IBM Spectrum Protect for Virtual Environments Data Protection for VMware para recuperar bancos de dados Microsoft SQL individuais a partir de um backup de máquina virtual. Ao recuperar um banco de dados, pode ser necessário solucionar problemas comuns que ocorrem com os bancos de dados SQL individuais.

Ao usar a proteção de aplicativo autocontida para Microsoft SQL no Data Protection for VMware, é possível fazer backup de uma máquina virtual guest que hospeda um aplicativo Microsoft SQL Server. Se você deseja restaurar um banco de dados Microsoft SQL individual a partir de um backup de máquina virtual, você deve usar IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server.

A tabela a seguir contém soluções para problemas comuns que você pode encontrar ao tentar recuperar os bancos de dados Microsoft SQL individuais a partir de um backup de máquina virtual.

Tabela 4. Informações de resolução de problemas para recuperação de banco de dados Microsoft SQL individuais a partir de um backup da máquina virtual

Problema	Solução ou Explicação
Não é possível acessar os backups de banco de dados com Proteção de Dados para SQL.	"Resolvendo Problemas de Acesso ao Banco de Dados" na página 51
É possível ver apenas as cópias inativas de bancos de dados SQL quando você usar a GUI de Proteção de Dados para SQL ou o comando <b>tdpsqlc</b> .	"Visualizando Cópias Ativas de Bancos de Dados Microsoft SQL" na página 52
Não é possível visualizar os nomes de banco de dados SQL que contêm caracteres do conjunto de caracteres de byte duplo (DBCS) com Proteção de Dados para SQL.	"Bancos de Dados Microsoft SQL com Nomes DBCS" na página 52
Você usou a proteção de aplicativo durante o backup de máquina virtual e recebeu mensagens de aviso e de erro.	"Respostas para Mensagens de Backups da Máquina Virtual com Proteção de Aplicativo" na página 53
Você deseja determinar quais bancos de dados SQL estavam na máquina virtual guest no momento de um backup da máquina virtual.	"Salvando Arquivos de Manifesto VSS XML" na página 53
Você deseja visualizar o status de gravadores VSS na máquina virtual guest.	"Determinando se um Backup de Máquina Virtual Pode Falhar" na página 54

# Resolvendo Problemas de Acesso ao Banco de Dados

Windows

Se você fez backup de uma máquina virtual guest que hospeda um aplicativo Microsoft SQL Server, talvez não seja possível acessar os bancos de dados com o Data Protection for SQL.

## Procedimento

Para resolver problemas de acesso ao banco de dados, conclua as seguintes etapas:

1. Verifique se a proteção de aplicativo foi usada quando você criou o backup de máquina virtual:

- a. A partir da janela Prompt de comandos, emita o seguinte comando do cliente de backup-archive para exibir a lista de backups de máquinas virtuais bem-sucedidos no servidor:

```
dsmc -node=datacenter_node query vm vm_name -detail
```

Onde *datacenter\_node* é o nome do nó virtual que retém os dados no centro e dados e *vm\_name* é o nome da máquina virtual submetida ao backup.

- b. Verifique se a saída deste comando contém os campos de saída a seguir:

```
application protection type: 'TSM VSS'
application(s) protected:    'MS SQL 2008 – database-level recovery'
```

Se a saída do comando não contiver esses campos de saída, ou o segundo campo não incluir o texto `database-level recovery`, conclua as etapas a seguir:

- 1) Assegure-se de que o cliente de backup-archive da V7.1 ou superior esteja instalado no nó do movedor de dados e de que o arquivo de opções do cliente contenha a opção `include.vmtsmvss vm_name`.
  - 2) Faça backup da máquina virtual guest novamente.
2. Verifique se o nome do computador da máquina virtual guest não foi alterada depois que o backup da máquina virtual foi criada.
  3. Verifique se o nó DSMAGENT in-guest possui acesso aos backups da máquina virtual do nó do datacenter.

- a. Emita o seguinte comando para verificar se o nó cliente tem acesso a versões de backup da máquina virtual no servidor:

```
dsmc -node=datacenter_node query access
```

Em que *datacenter\_node* é o nome do nó virtual que retém os dados no centro e dados.

- b. Verifique se a saída de comando contém os campos a seguir:

Type	Node	User	Path
Backup	<i>dsmagent_node</i>	*	\VMFULL- <i>vm_name</i> \*\*

Se a saída não contiver essas informações, execute novamente o comando **set access** no nó do movedor de dados para conceder ao nó DSMAGENT acesso aos backups da máquina virtual guest. Por exemplo, emita o comando a seguir:

```
dsmc set access backup -type=vm dsmagent_node vm_name
```

Em que *dsmagent\_node* é o nome do nó do cliente de backup-archive na máquina virtual guest, e *vm\_name* é o nome da máquina virtual que você submeteu a backup.

## O que Fazer Depois

Acesse os bancos de dados individuais com o Data Protection for SQL novamente.

## Visualizando Cópias Ativas de Bancos de Dados Microsoft SQL

Windows

Para conseguir visualizar as cópias ativas dos bancos de dados Microsoft SQL com Data Protection for SQL, você deve executar todos os backups incrementais primários e subsequentes dos bancos de dados SQL, usando Data Protection for VMware com proteção de aplicativos.

Se você usou a proteção de aplicativo para backup primário dos bancos de dados Microsoft SQL, mas não usou a proteção de aplicativo para backups incrementais subsequentes, nenhum backup ativo válido poderá ser usado para operações individuais de restauração de banco de dados SQL. A Proteção de Dados para SQL examina o backup da máquina virtual e pode exibir apenas os bancos de dados SQL dos backups de máquina virtual que foram submetidos a backup com êxito com proteção de aplicativo.

Assegure-se de ativar a proteção de aplicativo quando executar o backup primário e qualquer backup incremental subsequente da máquina virtual que hospeda o aplicativo Microsoft SQL. Este método assegura que as cópias ativas dos bancos de dados SQL que foram submetidos a backup a partir da máquina virtual podem ser exibidas pela Proteção de Dados para SQL.

## Bancos de Dados Microsoft SQL com Nomes DBCS

Windows

Enquanto o Data Protection for VMware estiver ativado para Unicode e puder fazer backup dos bancos de dados Microsoft SQL com nomes DBCS, a Proteção de Dados SQL não será ativada para Unicode. Portanto, não é possível usar a Proteção de Dados para SQL para restaurar bancos de dados com nomes DBCS a partir de uma máquina virtual que tenha sido submetida a backup com proteção de aplicativo.

Para restaurar um backup de máquina virtual que contém bancos de dados SQL com nome DBCS, você deve restaurar o backup de máquina virtual inteiro com Data Protection for VMware.

## Respostas para Mensagens de Backups da Máquina Virtual com Proteção de Aplicativo

Windows

Você pode receber alguns avisos ou mensagens de erro durante as operações de backup da máquina virtual quando usar a proteção de aplicativo.

As mensagens a seguir podem ser exibidas. Nesse caso, execute as ações a seguir:

**ANS2196W Uma configuração de disco incompatível é detectada. A restauração de Banco de Dados SQL Individual do banco de dados '<database\_name>' não é suportada.**

É possível usar os bancos de dados Microsoft SQL que estão em discos básicos com particionamento Master Boot Record (MBR) para recuperação de banco de dados SQL individual. Essa mensagem de aviso identifica um ou mais bancos de dados SQL que possuem uma configuração de disco não suportada.

**ANS2330E A falha ao descongelar os gravadores VSS devido ao tempo de captura instantânea excedeu a limitação de tempo limite de 10 segundos.**

Determine se existe um erro, executando as ações a seguir:

1. Use o cliente vSphere para criar uma captura instantânea de máquina virtual em modo quiesce. Se esta ação for bem-sucedida, continue na próxima etapa.

Se esta ação não for bem-sucedida, o problema provavelmente está relacionado ao VMware. Pode ser necessário entrar em contato com o Suporte VMware a respeito do problema.

2. Faça backup da máquina virtual sem proteção de aplicativo:
  - a. Desative a proteção de aplicativo removendo a opção `INCLUDE.VMTSMVSS vmname` do arquivo de opções do cliente.
  - b. Faça backup da máquina virtual executando o seguinte comando a partir da janela Prompt de comandos:

```
dsmc backup vm vmname -vmbackuptype=fullvm
```

Em que *vmname* é o nome da máquina virtual em que você deseja fazer backup.

As etapas seguidas até agora podem ajudá-lo a melhor diagnosticar e resolver o problema. No entanto, se esta etapa não for bem-sucedida, existe um problema com a máquina virtual guest do Windows ou o cliente de backup-archive no nó do movedor de dados. Pode ser necessário localizar informações de suporte para IBM Spectrum Protect no IBM Portal de Suporte para IBM Spectrum Protect.

## Salvando Arquivos de Manifesto VSS XML

Windows

Salvar os arquivos de manifesto VSS XML pode ajudar na determinação de quais bancos de dados Microsoft SQL foram localizados na máquina virtual guest no momento do backup.

## Sobre Esta Tarefa

Os arquivos de manifesto VSS XML contêm informações do gravador VSS geradas durante a operação de backup da máquina virtual. Os arquivos de manifesto VSS XML são necessários para operações de restauração VSS dos bancos de dados Microsoft SQL selecionados.

## Procedimento

Para salvar os arquivos de manifesto VSS XML no nó do movedor de dados, conclua as etapas a seguir:

1. Inclua a instrução a seguir no arquivo de opções do cliente:  
`testflag VMBACKup_SAVE_LOCAL`
2. Inicie um backup da máquina virtual com proteção de aplicativo da máquina virtual guest que hospeda o aplicativo SQL Server.

Depois que a operação de backup da máquina virtual for concluída, os arquivos de manifesto VSS XML são salvos para o local a seguir no nó do movedor de dados.

```
C:\mnt\tsmvmbackup\fullvm\vm_tsmvss\vm_name
```

Em que *vm\_name* é o nome da máquina virtual que tem o backup feito.

3. Visualize a lista de bancos de dados SQL que são localizados na máquina virtual guest no momento do backup abrindo o arquivo `sqldbinfo.xml` com um editor de texto. Assegure-se de que o arquivo `sqldbinfo.xml` contém as informações completas sobre os bancos de dados SQL que foram submetidos a backup.

## Determinando se um Backup de Máquina Virtual Pode Falhar

### Windows

Verifique o status dos gravadores VSS em uma máquina virtual guest para determinar se um backup de máquina virtual com a proteção de aplicativo pode falhar.

## Sobre Esta Tarefa

Use o comando **vssadmin list writers** para exibir o status dos gravadores VSS. Este comando lista todos os gravadores que estão disponíveis na máquina virtual guest, incluindo o status dos gravadores. Se um ou mais dos gravadores VSS não estiverem em um estado estável, o backup da máquina virtual com a proteção de aplicativo falhará.

## Procedimento

Na janela Prompt de Comandos, emita o comando a seguir:

```
vssadmin list writers
```

A amostra a seguir mostra a saída de comando:

```
Writer name: 'SqlServerWriter'
  Writer Id: {a65faa63-5ea8-4ebc-9dbd-a0c4db26912a}
  Writer Instance Id: {debc861a-7709-48b4-86a5-0a62457dc4a0}
  State: [1] Stable
  Last error: No error
```



O campo Estado indica o status do gravador VSS.



---

## Capítulo 3. Resolvendo problemas do servidor IBM Spectrum Protect

Ao trabalhar com o IBM Spectrum Protect, você pode ter problemas específicos com o servidor. As dicas de diagnósticos do servidor que você pode executar variam de ações simples, como reiniciar o servidor, a procedimentos com maior envolvimento.

A lista a seguir contém algumas ações que podem ser executadas para ajudar a diagnosticar problemas do servidor:

- Recriar o problema
- Verificar o log de atividade do servidor e outros logs
- Verificar logs de erros relacionados à leitura ou gravação em um dispositivo
- Alterar as opções do servidor
- Parar e iniciar serviços de planejamento
- Consultar o banco de dados ou o conjunto de armazenamentos
- Rastrear a classe de rastreo UNICODE

---

### Recriando o Problema

Recrie o problema para isolar sua causa para uma sequência específica de eventos, se o problema puder ser recriado de maneira fácil ou consistente.

Muitos problemas ocorrem como resultado de uma combinação de eventos. Por exemplo, a expiração em execução com backups planejados no período noturno para 20 clientes. Em alguns casos, mudando a sincronização ou a ordem da implementação de eventos, você pode evitar que o problema ocorra novamente. Uma forma de alterar a sincronização é executar a expiração em um horário no qual os backups planejados no período noturno para 20 clientes não estejam executando.

---

### Verificando o arquivo de log de atividade do servidor e outros arquivos de log

Verifique o arquivo de log de atividade do servidor e consulte relatórios de 30 minutos antes e 30 minutos depois do momento do erro.

Para revisar as mensagens no log de atividades do servidor, emita o comando **QUERY ACTLOG**. Geralmente, outras mensagens podem oferecer informações adicionais sobre a causa do problema e como resolvê-lo.

#### Lista de arquivos de log adicionais

O Suporte de Software IBM pode solicitar que sejam enviados os seguintes arquivos de log:

- Arquivos de log do servidor da web:
  - console.log
  - messages.log
- Arquivos de log de primeira captura de dados com falha (FFDC):
  - exception\_summary\_date\_time.log

– `ffdc_date_time.log`

### Local de Arquivos de Log

- Os arquivos de log do servidor da web estão no seguinte diretório:

**AIX**   **Linux**   `installation_dir/ui/Liberty/usr/servers/guiServer/logs`

**Windows**   `installation_dir\ui\Liberty\usr\servers\guiServer\logs`

em que *installation\_dir* representa o diretório no qual o IBM Spectrum Protect está instalado. Por exemplo:

**AIX**   **Linux**   `/opt/tivoli/tsm`

**Windows**   `c:\Program Files\Tivoli\TSM`

- Os arquivos de log FFDC estão no mesmo local, mas no subdiretório `ffdc`.

---

## Verificando Erros de Dispositivo em Arquivos de Log de Erro de Sistema

Se o problema for um erro criado ao ler ou gravar dados de um dispositivo, muitos sistemas e dispositivos registram informações em um log de erro de sistema.

Se um dispositivo ou volume que está sendo usado pelo IBM Spectrum Protect estiver relatando algum tipo de erro no log de erro de sistema, provavelmente será um problema do dispositivo. As mensagens de erro registradas no log de erro de sistema podem fornecer informações suficientes para resolver o problema.

A seguir, alguns exemplos de logs de erro do sistema:

- `errpt` para AIX
- Log de Eventos para Windows

---

## Revertendo Opções ou Configurações do Servidor

Caso tenha ocorrido alguma mudança na configuração do servidor, tente voltar as configurações aos seus valores originais e tente novamente a operação que falhou.

Se a operação for bem-sucedida, tente fazer uma mudança por vez e tente novamente a operação até que a mudança de atributo que causou a falha seja identificada.

As mudanças nas opções no arquivo de opções do servidor, ou alterações na configuração para o servidor usando os comandos **SET** ou **UPDATE** podem causar falhas para operações que foram bem-sucedidas anteriormente. As mudanças no servidor para classes de dispositivo, conjuntos de armazenamentos e políticas também podem causar falhas em operações que foram bem-sucedidas anteriormente.

---

## Reiniciando o Serviço de Planejamento

As opções do cliente planejadas são influenciadas pelas definições de planejamento no servidor, bem como o serviço de planejamento (dsmsched) executado no próprio computador do cliente.

Reinicie o serviço de planejamento no cliente se um planejamento for alterado no servidor.

**Importante:** Se o serviço de planejamento for gerenciado pelo aceitante do cliente, pare e reinicie apenas o aceitante do cliente.

---

## Resolvendo Problemas de Espaço do Servidor

A função primária do servidor IBM Spectrum Protect é armazenar dados. Se não houver espaço no banco de dados ou nos conjuntos de armazenamentos, as operações poderão falhar.

Para determinar se o banco de dados está sem espaço, emita o comando **QUERY DB**. Se o percentual utilizado (espaço usado) estiver em ou próximo de 100%, defina mais espaço. Geralmente, se o banco de dados estiver executando sem espaço, essa situação será indicada por outras mensagens emitidas do servidor.

Para determinar se um conjunto de armazenamentos está sem espaço, emita o comando **QUERY STGPOOL**. Se o percentual utilizado estiver em ou próximo de 100%, disponibilize mais espaço de armazenamento. Para incluir mais espaço em um conjunto de armazenamentos em DISCO, aloque um ou mais novos conjuntos de armazenamentos e os defina para o servidor usando o comando **DEFINE VOLUME**. É possível configurar o IBM Spectrum Protect para alocar automaticamente o espaço em DISCO e de ARQUIVO do conjunto de armazenamentos usando o comando **DEFINE SPACETRIGGER**.

Para incluir mais espaço em um conjunto de armazenamentos de mídia sequencial, avalie a biblioteca de fitas e determine se é possível incluir mais fitas utilizáveis. Neste caso, inclua os volumes utilizáveis adicionais na biblioteca e atualize o parâmetro **MAXSCR** para o conjunto de armazenamentos emitindo o comando **UPDATE STGPOOL**.

---

## Alocando Memória Adicional do Servidor

Aloque mais memória no servidor se houver indicações de que o servidor está com baixos recursos de memória. Consulte a documentação do seu sistema operacional para obter informações sobre como incluir memória.

**Dica:** A quantidade de memória que o DB2 usa pode contribuir com os relatórios que mostram que o sistema operacional está sem memória. Você pode limitar a quantidade de memória que o DB2 usa incluindo a opção **DBMEMPERCENT**. A opção **DBMEMPERCENT** especifica a porcentagem de espaço de endereço virtual que está dedicada aos processos do gerenciador de banco de dados.

Execute as ações a seguir para alocar recursos adicionais de armazenamento para o servidor:

- **AIX** Certifique-se de que existe espaço de paginação suficiente. Você também pode usar SMIT (System Management Interface Tool) para determinar se o número de aplicativos está causando uma insuficiência de memória.

- **Windows** O método preferido de resolver uma condição de memória baixa é incluir memória física no sistema. Caso contrário, no painel de controle, aumente a quantidade do armazenamento virtual executando o applet do sistema e aumentando o tamanho total do arquivo de paginação.

---

## Configurando uma Instância do Servidor para Usar Memória Compartilhada

Configure uma instância de servidor para usar a memória compartilhada para ajudar a resolver backups de banco de dados lentos, que podem ocorrer devido a problemas de loopback do Protocolo de Controle de Transmissões (TCP).

### Sobre Esta Tarefa

No procedimento a seguir, você deve atualizar a configuração do nó de backup de banco de dados para seu servidor para ativar a memória compartilhada.

- **AIX** **Linux** `server_bin_directory/dbbkapi/dsm.sys`
- **Windows** `server_instance_directory\tsmdbmgr.opt`

### Procedimento

1. Certifique-se de que o arquivo de opções do servidor, `dsmerv.opt`, contenha as seguintes linhas:

```
COMMMethod          SHAREdmem
SHMPort             1510
```

2. **AIX** **Linux** Modifique a sub-rotina para o nó de backup de banco de dados no arquivo de opções do sistema da API do cliente, `dsm.sys`.

- Remova as seguintes linhas da sub-rotina:

```
COMMMethod          TCPip
TCPServeraddress 127.0.0.1
TCPPort            1500
```

- Inclua as seguintes linhas na sub-rotina:

```
COMMMethod          SHAREdmem
SHMPort 1510
```

3. **Windows** Modifique a sub-rotina para o nó de backup do banco de dados no arquivo de opções do sistema da API do cliente, `tsmdbmgr.opt`.

- Remova as seguintes linhas do arquivo `tsmdbmgr.opt`:

```
COMMMethod          TCPip
TCPServeraddress 127.0.0.1
TCPPort            1500
```

- Inclua as seguintes linhas no arquivo `tsmdbmgr.opt`:

```
COMMMethod          SHAREdmem
SHMPort 1510
```

---

## Alterando a Frequência de Cópia

A política do servidor IBM Spectrum Protect demanda que uma frequência de cópia incremental seja um valor diferente de zero.

O atributo de frequência de cópia da classe de gerenciamento *copygroup* atual para o arquivo especificado dita o número mínimo de dias que devem decorrer entre backups incrementais sucessivos. Se você estiver tentando executar um backup incremental de um arquivo e esse número estiver configurado como maior que 0 dias, o arquivo não será enviado para o servidor, mesmo se ele tiver sido mudado.

Podem ser executadas várias etapas para corrigir este problema:

- Entre em contato com o administrador do servidor para mudar o atributo de frequência de cópias.
- Emita um backup seletivo do arquivo. Por exemplo, DSMC SELECTIVE C:\FILE.TXT

É possível emitir o comando **QUERY COPYGROUP** para determinar a configuração do parâmetro de frequência de cópia:

```
tsm: WINBETA>q copygroup standard active f=d
Policy Domain Name: STANDARD
...
Copy Frequency: 1
...
```

---

## Resolvendo Erros de Operação RELABEL

Se você executar uma operação RELABEL quando todas as unidades estiverem ocupadas, o volume de destino não poderá ser novamente rotulado porque ele não pode obter uma unidade. Unidades ocupadas são unidades que estão sendo usadas para operações comuns, como backup, restauração, migração e recuperação.

Quando ocorre um erro RELABEL, as seguintes informações de exemplo são produzidas:

```
ANR0984I Process 25 for RELABEL started in the BACKGROUND at 22:10:36.
ANR8799I RELABEL: Operation for library IBMVTI started as process 25.
ANR1341I Scratch volume 007403 has been deleted from storage pool VTLP00L.
ANR8847E No LTO-type drives are currently available in library IBMVTI.
ANR8801I LABEL LIBVOLUME process 25 for library IBMVTI completed; 0 volume(s)
labeled, 0 volume(s) checked-in.
ANR0985I Process 25 for RELABEL running in the BACKGROUND completed with
completion state SUCCESS at 22:10:36.
```

Para resolver um erro RELABEL, conclua as seguintes etapas:

1. Verifique se uma unidade está mantida disponível para a operação RELABEL e rotule novamente um volume de destino.
2. Atualize as classes de dispositivo que apontam para a biblioteca. Atualize as classes de dispositivo com um valor de parâmetro **MOUNTLIMIT** que seja inferior ao número total de unidades disponíveis.

Se uma operação RELABEL não puder obter uma unidade ou falhar ao rotular um volume novamente, o IBM Spectrum Protect tentará rotulá-lo novamente durante cada operação RELABEL futura.

Se a operação RELABEL falhar, emita o comando **LABEL LIBVOLUME** para todos os volumes que são retirados do IBM Spectrum Protect mas que não são novamente rotulados. Inclua os seguintes parâmetros no comando **LABEL LIBVOLUME**:

---

## Evitando Erros de Comunicação Durante o Processamento de Importação

Os erros de comunicação são exibidos no log de atividades do servidor de destino se você cancelar o processo de importação do servidor de destino.

Se você cancelar o processo de importação a partir do servidor de destino, as mensagens de erro de comunicação no log de atividades mostrarão o nome do nó que iniciou a operação de exportação a partir do servidor de origem. Por exemplo, as mensagens a seguir podem ser exibidas no log de atividades do servidor:

```
ANR0440W Protocol error on session 2 for node ADMIN
ANR3174E Communication error with managed server ADMIN.
ANR0484W Session 2 for node ADMIN terminated - protocol violation detected.
```

É possível ignorar as mensagens de erro de comunicação no log de atividades do servidor de destino que pertence ao processo de importação. Como alternativa, se você cancelar o processo de importação do servidor de origem, nenhuma mensagem de erro de comunicação ocorrerá no servidor de origem ou de destino.

---

## Incluindo um certificado autoassinado para o keystore

É possível configurar comunicações seguras usando um certificado autoassinado com seu sistema de armazenamento de objetos. Nesta situação, o IBM Spectrum Protect usa HTTPS em vez de HTTP ao se comunicar com o sistema de armazenamento de objetos. As etapas a seguir fornecem um método para importar certificados.

### Sobre Esta Tarefa

Utilize um navegador da web para obter uma cópia do certificado utilizado pelo sistema de armazenamento de objetos. As etapas a seguir são específicas para Firefox, mas outros navegadores fornecem funções semelhantes. Consulte as instruções de seu navegador preferido sobre a exportação de certificados.

### Procedimento

1. Obtenha o certificado usado pelo servidor OpenStack Swift ou o IBM Cloud Object Storage.
  - a. Digite a URL para seu sistema de armazenamento de objetos na barra de endereços do navegador e pressione **Enter**. Use a URL do servidor Keystone for OpenStack ou a URL do nó acessador para IBM Cloud Object Storage.

**Dica:** se você estiver usando o IBM Cloud Object Storage como o sistema de armazenamento de objeto, efetue login no IBM Cloud Object Storage e clique na guia **Segurança**. Na seção **Impressão Digital dsNet**, clique em **Autoridade de certificação dsNet** e copie as informações do certificado em um arquivo de certificado para a Parte 2.
  - b. Aceite todos os avisos exibidos pelo navegador.
  - c. Clique no ícone de bloqueio na barra de endereços do navegador.
  - d. Selecione **Mais informações** na janela pop-up.
  - e. Selecione **Visualizar certificado** na janela Informações de página.
  - f. Clique na guia **Detalhes** na página Visualizador de certificado e, em seguida, selecione **Exportar**.



- g. Salve o arquivo exportado para o local que você deseja.
- 2. Inclua o certificado no Keystore padrão do Java.

As etapas a seguir supõem que os nós clientes estejam no Linux, e que o servidor esteja em execução no Linux. Como cada acessador do IBM Cloud Object Storage possui seu próprio certificado por padrão, inclua o certificado para cada acessador no Keystore e utilize um alias diferente para cada certificado.

  - a. Abra um terminal e mude o diretório para o diretório jre/bin.

O local de instalação padrão é /opt/tivoli/tsm/jre/bin.
  - b. Faça uma cópia de backup do arquivo cacerts do Java executando o comando a seguir: `cp ../lib/security/cacerts ../lib/security/cacerts.original`.

Em um sistema Windows, o local do Keystore cacerts do Java é: `install_dir\jre\lib\security\`, e o local do Keytool é `install_dir\jre\bin\`.
  - c. Importe o certificado salvo do procedimento anterior executando o seguinte comando: `./keytool -import -keystore ../lib/security/cacerts -alias somealias -file yourfile`

em que *somealias* é um alias exclusivo para esse certificado no keystore, que será importante se você possuir mais de um certificado, e *yourfile* é o caminho e o nome de arquivo do certificado da primeira etapa dessas instruções.
  - d. Quando for solicitado a fornecer a senha, digite *changeit*. Se você mudou sua senha da senha padrão, digite a senha atual.
  - e. Quando você for solicitado a confiar nesse certificado, digite *yes*.

A mensagem a seguir é mostrada quando o certificado é incluído com êxito: Certificate was added to keystore. Os certificados padrão possuem uma expiração curta. Quando eles expiram, você pode perder o acesso ao armazenamento de objetos, até que atualize os certificados. É possível criar seus próprios certificados e usá-los, mas criar e instalar tais certificados nos sistemas de armazenamento de objetos está fora do escopo deste documento.
  - f. Reinicie o servidor IBM Spectrum Protect.

---

## Determinando por que os registros de resumo para um evento de backup do cliente estão ausentes

Se uma sessão de comunicação entre o servidor e o cliente for encerrada de forma anormal, pode haver um atraso antes de os registros de resumo para um evento de backup do cliente serem incluídos no banco de dados do servidor.

### Sintoma

Após a conclusão de um processo de backup de cliente, o registro não é incluído no banco de dados imediatamente. Pode levar várias horas para que o registro de resumo seja incluído no banco de dados.

## Causas

Pode levar várias horas para que os registros de resumo sejam incluídos no banco de dados do servidor, porque uma sessão do servidor deve aguardar a conclusão do processamento de encerramento anormal. Uma sessão pode ser encerrada de forma anormal pelas seguintes razões:

- Falhas de rede
- Tempos limites da sessão

Os tempos limite da sessão podem ocorrer quando os processos de backup demoram mais que o esperado.

## Resolvendo o Problema

1. Para determinar por que as sessões de comunicação entre o servidor e o cliente foram encerradas de forma anormal, execute as seguintes ações:
  - a. Revise o log de atividades emitindo o comando **QUERY ACTLOG**.
  - b. Revise o log de erro do cliente, `dsmerror.log`, no diretório de instalação do cliente.
  - c. Se não for possível determinar a causa do problema revisando a atividade do log, ative o rastreo para o cliente de backup-archive.
2. Resolva os problemas de comunicação. É possível trabalhar com sua equipe de rede para coletar e analisar dados da rede.

### Referências relacionadas:

“Ativando o Rastreo do Cliente de Backup-archive” na página 160

---

## Resolvendo Problemas de Instalação e Upgrade

A resolução de problemas de instalação com o servidor IBM Spectrum Protect pode envolver a revisão de arquivos de log, a reinstalação do servidor ou várias outras opções possíveis.

## Arquivos de Log de Instalação

Se ocorrerem erros durante o processo de instalação, esses erros são registrados nos arquivos de log.

Para visualizar arquivos de log de instalação, clique em **Arquivo > Visualizar Log** da ferramenta Gerenciador de Instalação. Para coletar esses arquivos de log, clique em **Ajuda > Dados de Exportação para Análise de Problemas** a partir da ferramenta Installation Manager.

Os arquivos de log são armazenados no diretório de logs do IBM Installation Manager:

AIX	Linux	/var/ibm/InstallationManager/logs
Windows		C:\ProgramData\IBM\Installation Manager\logs

## O Assistente de Instalação Falha ao Iniciar

O IBM Installation Manager requer bibliotecas gtk para suportar a interface gráfica com o usuário (GUI) em sistemas AIX. Se essas bibliotecas não forem instaladas antes da instalação do servidor IBM Spectrum Protect, a instalação não poderá ser iniciada. É emitido um erro sobre bibliotecas gtk ausentes.

**Informações relacionadas:**



Instalando o IBM Spectrum Protect usando o assistente de instalação

## Resolvendo Problemas de Instalação de GSKit

Quando você usa o software de instalação do IBM Spectrum Protect, a versão correta do Global Security Kit (GSKit) é instalada automaticamente.

Se o ambiente de instância do servidor IBM Spectrum Protect não estiver corretamente configurado, o servidor poderá não carregar as bibliotecas GSKit adequadas. O assistente de configuração de instância do servidor o ajuda a evitar muitos problemas que possam ser predominantes ao configurar manualmente a instância.

**Windows**

Emita o seguinte comando:

```
set PATH=X:\Program Files\IBM\gsk8\bin;X:\Program Files\IBM\gsk8\lib64;%PATH%
```

em que X é a unidade de sistema. A variável de ambiente PATH é modificada para apontar para o diretório correto.

**Linux**

Atualize o LD\_LIBRARY\_PATH ou shell emitindo o seguinte comando:

```
export LD_LIBRARY_PATH=platform-specific-gskit-library-directory:$LD_LIBRARY_PATH
```

em que *platform-specific-gskit-library-directory* é um desses diretórios, de acordo com sua plataforma:

- **Linux** /usr/local/ibm/gsk8\_64/lib64

**AIX**

Para AIX, emita o seguinte comando:

```
export LIBPATH=/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

**AIX**

**Linux**

Você deve atualizar os seguintes arquivos para configurar o caminho da biblioteca quando o DB2 ou o servidor for iniciado:

- *instance\_directory/sqllib/usercshrc*
- *instance\_directory/sqllib/userprofile*

Para o arquivo *instance\_directory/sqllib/usercshrc*, inclua as seguintes linhas:

- **AIX**

```
setenv LIBPATH /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

- **Linux**

```
setenv LD_LIBRARY_PATH /usr/local/ibm/gsk8_64/lib64:$LD_LIBRARY_PATH
```

Para o arquivo *instance\_directory/sqllib/userprofile*, inclua as seguintes linhas:

- **AIX**

```
LIBPATH=/usr/opt/ibm/gsk8_64/lib64:$LIBPATH  
export LIBPATH
```

- **Linux**

```
LD_LIBRARY_PATH=/usr/local/ibm/gsk8_64/lib64:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
```

Verifique as configurações do caminho da biblioteca e a versão do GSKit emitindo os seguintes comandos:

- **AIX**  

```
echo $LIBPATH
gsk8capicmd_64 -version
```
- **Linux**  

```
echo $LD_LIBRARY_PATH
gsk8ver_64
```

Se a versão do GSKit não for 8.0.14.28 ou posterior, deverá reinstalar o servidor. A reinstalação assegura que a versão correta do GSKit está disponível.

## Instâncias de Serviço Não Criadas Durante um Upgrade

Quando uma conexão não pode ser estabelecida, o instalador não pode recriar suas instâncias do servidor IBM Spectrum Protect. Você deve recriá-las manualmente.

### Sobre Esta Tarefa

O assistente de instalação usa os seguintes métodos para estabelecer uma conexão com o sistema para recriar as instâncias do servidor:

- **AIX** **Linux** Secure shell (SSH)
- **Windows** Bloco de mensagens do servidor (SMB) Windows

Quando você usa um desses métodos na porta padrão, a porta não pode ser bloqueada por um firewall. Se estiver bloqueado, conclua as seguintes etapas para fazer upgrade manualmente da instância do servidor. **AIX** **Linux**

### Procedimento

1. Feche o assistente de instalação.
2. Conclua as seguintes etapas para cada instância do servidor:
  - a. Depois de concluir o upgrade, emita o comando a seguir para recriar a instância:

```
/opt/tivoli/tsm/db2/instance/db2icrt -u instance_user
instance_name
```
  - b. Recrie as variáveis no arquivo de instância. Emita o comando **db2set -i** para cada variável no arquivo de instância. Por exemplo, configure a variável **DB2COMM** para que seja apenas TCPIP para a instância MYINST:

```
/opt/tivoli/tsm/db2/instance/db2set -i MYINST DB2COMM=TCPIP
```

Para exibir uma lista de todas as variáveis definidas, especifique o parâmetro **-all**, por exemplo, **db2set -all**.
  - c. Emita o comando **db2stop** para parar a instância do banco de dados.
  - d. Use o ID do usuário que possua a instância do servidor para emitir o comando **db2start** para iniciar a instância do banco de dados.
  - e. Catalogue e atualize cada banco de dados emitindo os seguintes comandos:

```
db2 catalog db TSMDB1 on "database_path"
db2 upgrade db TSMDB1
```
  - f. Emita o comando **db2stop**.
  - g. Inicie o servidor.

## Resolvendo um Processo de Desinstalação Interrompido

Uma senha de usuário da instância do DB2 expirada pode causar a parada do processo de desinstalação do IBM Spectrum Protect antes de sua conclusão.

Se a senha do ID do usuário da instância do DB2 estiver expirada, o processo de desinstalação não poderá ser concluído. Você deve efetuar login usando o ID do usuário da instância do DB2 e reconfigurar a senha, em seguida, desinstalar o IBM Spectrum Protect.

## A Implementação Automática do Cliente não Fez Upgrade do Software Cliente

Se o planejamento de implementação for concluído, mas não for feito upgrade do software cliente para o nível de destino, revise os arquivos de log no sistema do cliente.

### Sintoma

Não foi feito upgrade do software cliente para o nível de destino após a conclusão do planejamento da implementação automática.

### Causa

Os exemplos a seguir são alguns motivos pelos quais o software cliente não faz upgrade para o nível de destino.

- Não há espaço suficiente no sistema de arquivos do cliente para concluir o upgrade.
- Problemas de rede impediram que os dados do servidor fossem transferidos para o sistema do cliente.

### Resolvendo o Problema

É possível resolver a falha de upgrade do cliente, revisando os arquivos de log e de rastreamento no sistema do cliente. O gerenciador de implementação grava os dados de log e rastreamento de uma operação de implementação no sistema de arquivos do cliente. O local para os arquivos de log é especificado na definição de planejamento de implementação no servidor.

Conclua as seguintes etapas para resolver a falha de upgrade do cliente:

1. Altere os diretórios para o local dos arquivos de log.
  - **AIX** O local padrão é /usr/tivoli/client/IBM\_ANR\_UNX/Vxxxx/log.
  - **Linux** O local padrão é /opt/tivoli/tsm/client/IBM\_ANR\_UNX/Vxxxx/log.
  - **Mac OS X** O local padrão é /Library/Application Support/tivoli/tsm/client/ba/bin/IBM\_ANR\_MAC/Vxxxx/log.
  - **Windows** O local padrão é C:\Program Files\Tivoli\TSM\IBM\_ANR\_WIN\Vxxxx\log.

Em que o diretório Vxxxx no caminho representa o nível de destino do cliente de backup-archive implementado.

2. Revise os arquivos de log e de rastreamento do gerenciador de implementação para determinar a causa raiz da falha de upgrade do cliente. A Tabela 5 na página 68 mostra uma lista de arquivos de log possíveis de revisar.

Tabela 5. Descrição de arquivos de log

Nome do log	descrição
setup.log	P log de erro que mostra mensagens de erro, de aviso e informativas.
trace.txt	Rastreio do cliente que mostra informações detalhadas sobre o processo de upgrade do cliente.
updatemgr.log	Log do gerenciador de implementação que mostra informações sobre o processo de implementação.

## Resolvendo Interrupções do Servidor

As interrupções do servidor podem ocorrer de erros de processamento, do manipulador de trap do sistema ou de outros erros. Ao determinar a origem da interrupção do servidor, a razão poderá resolver outros problemas conhecidos.

O servidor pode parar por uma das seguintes razões:

- Um erro de processamento faz a memória ser sobrescrita ou algum outro evento acionar o manipulador de trap do sistema para terminar o processo do servidor.
- O processo do servidor possui algoritmos de validação em todo o aplicativo, que verificam diversas condições antes de continuar a execução. Como parte desta verificação de validação, existem casos em que, se a verificação da validação falhar, o servidor terminará a si mesmo, em vez de permitir que o processamento continue. Estas validações catastróficas são referidas como uma afirmação. Se o servidor terminar devido a uma asserção, a seguinte mensagem será exibida:

ANR7837S Detectado erro interno XXXNNN.

em que XXXNNN é um identificador designado à falha de asserção.

Outras mensagens do servidor que são indicativas de uma interrupção são ANR7836S e ANR7838S.

Se o servidor tiver sido interrompido como resultado de uma asserção ou do manipulador de trap do sistema, o utilitário tsmdiag poderá coletar as informações a seguir e compactá-las para envio para o serviço IBM para que a situação possa ser diagnosticada:

- Arquivo de erro do servidor (dsmserv.err)
- Imagem do sistema (arquivo de núcleo)
- Bibliotecas e outros arquivos
- Logs do sistema
- Log de Atividade

Compacte todos os dados (arquivos) coletados e entre em contato com o serviço IBM para relatar esse problema.

### Tarefas relacionadas:

Apêndice B, “Executando o Utilitário tsmdiag”, na página 211

## Resolvendo uma Interrupção ou Loop

Uma interrupção é uma situação na qual o servidor não inicia nem conclui uma função e não está usando nenhuma energia do microprocessador.

Uma interrupção pode ser apenas uma sessão ou processo que não está sendo processado, ou pode ser o servidor IBM Spectrum Protect inteiro que não está respondendo. Um loop é uma situação na qual nenhum progresso está sendo feito, mas o servidor está usando uma grande quantidade de energia do microprocessador. Um loop pode afetar apenas uma sessão ou um processo ou pode afetar o servidor inteiro.

É possível coletar a documentação para resolver este tipo de problema, caso o servidor possa responder a comandos. Um script Perl está disponível para você coletar dados do servidor. É útil planejar a lista de comandos **SHOW** para execução intermitente para que seja possível ver o comportamento que precede a situação de interrupção.

- Para uma interrupção ou um loop no qual o servidor pode responder a comandos, emita os seguintes comandos para ajudar a determinar a causa da interrupção:
    - **QUERY SESSION f=d**
    - **QUERY PROCESS**
    - **SHOW RESQ**
    - **SHOW THREADS**
    - **SHOW DEADLOCK**
    - **SHOW TXNT**
    - **SHOW DBTXNT**
    - **SHOW LOCKS**
    - **SHOW LIBR**
    - **SHOW MP**
    - **SHOW SESS**
    - **SHOW ASQ**
    - **SHOW ASVOL**
    - **SHOW DBV**
    - **SHOW SSS**
    - **SHOW CSV** (Emita esse comando apenas quando o problema estiver relacionado ao planejamento.)
  - Quando um servidor é interrompido ou entra em loop, emita os seguintes comandos para fornecer uma captura instantânea de diagnóstico detalhada do ambiente do IBM Spectrum Protect:

```
db2fodc -hang -alldbs
db2support . -d database -s
```
- É possível usar o arquivo `db2support.zip` gerado para a resolução de problemas.
- Além da saída dos comandos listados, ou no caso de um servidor que não pode responder a comandos, colete um dump. A maneira de coletar um dump depende do sistema operacional.
    - **AIX** **Linux** Emita o comando **KILL -11** no processo `dsmserv` para criar um arquivo principal. Para executar o comando “kill”, obtenha o ID do processo, emitindo o comando **PS**.

- **Windows** Procure coletar dumps de modo de usuário no website da Microsoft em <http://support.microsoft.com/>.

## Resolvendo Problemas de Estado de Espera com Servidores de Repositório do Usuário Externo

Se o servidor IBM Spectrum Protect parece não responsivo, isso pode estar relacionado ao sistema operacional e ao uso pelo sistema operacional de um repositório do usuário externo.

### Antes de Iniciar

O desempenho lento do servidor pode ser atribuído a um sistema operacional que usa um repositório de usuário externo que tem muitos grupos de usuários definidos. Servidores NIS (Serviço de Informações de Rede) e LDAP (Protocolo LDAP) são dois tipos de servidores de repositório do usuário externo.

Um exemplo do comportamento não responsivo é quando o IBM Spectrum Protect demora muito para se conectar ao servidor IBM DB2. Outro exemplo é quando o servidor parece não responsivo para solicitações administrativas.

### Sobre Esta Tarefa

Conclua as etapas a seguir para resolver um problema de estado de espera que ocorre com os servidores a seguir quando você estiver usando um servidor LDAP:

### Procedimento

1. Pare o servidor IBM Spectrum Protect.
2. **AIX** Emita os seguintes comandos:
  - a. `db2set DB2_ALTERNATE_GROUP_LOOKUP=GETGRSET`
  - b. `db2stop force`
  - c. `db2start`**Linux** Emita os seguintes comandos:
  - a. `db2set DB2_ALTERNATE_GROUP_LOOKUP=GETGROUPLIST`
  - b. `db2stop force`
  - c. `db2start`
3. Reinicie o servidor.

## Localizando o Arquivo de Erros do Servidor (dsmserv.err)

Quando o servidor para, ele anexa informações ao arquivo `dsmserv.err`, que está localizado no mesmo diretório que o servidor.

### Antes de Iniciar

**AIX** **Linux** O manipulador de trap é desativado para evitar que a análise retrospectiva da função seja impressa no console e no arquivo `dsmserv.err`. Esta mudança é necessária para assegurar que será obtido um dump de núcleo mais completo. Como parte da desativação do manipulador de trap, um novo script, `getcoreinfo`, está nos pacotes do Linux. O script `getcoreinfo` obtém a análise retrospectiva de função para o encadeamento com falha e registra valores e análise retrospectiva de função para todos os demais encadeamentos. A quantidade de informações disponíveis no núcleo para outros encadeamentos ainda está



incompleta em algumas plataformas/distribuições Linux. Consulte o script `getcoreinfo` (no diretório `bin` do servidor) para obter mais detalhes.

**Windows** Se o servidor estiver em execução como um serviço, o arquivo será denominado `dsmsvc.err`.

## Sobre Esta Tarefa

Execute as seguintes etapas para capturar o arquivo de erros do servidor:

### Procedimento

1. Certifique-se de que o depurador GNU (gdb) esteja instalado no sistema do cliente.
2. Copie o script de shell `gt` para o diretório `bin` do servidor (onde o arquivo executável do servidor `[.exe]` e o dump de núcleo estão localizados).
3. Certifique-se de que o script seja um arquivo executável (`chmod a+x gt`).
4. Invoque o script com os caminhos/nomes do arquivo executável (o padrão é `./dsmserv`) e o núcleo (o padrão é `./dsmcore`). A saída está no arquivo `dsm_gdb.info` (que deve ser enviado para IBM).

## Localizando a Imagem do Sistema (Arquivo de Núcleo)

Geralmente, um arquivo de núcleo ou outra imagem do sistema da memória está sendo usado pelo IBM Spectrum Protect no momento da falha.

Em cada caso, renomeie o arquivo principal para impedir que ele seja sobrescrito por uma interrupção posterior. Por exemplo, um arquivo deve ser renomeado para `"core.Aug29"` em vez de `"core."` O tipo e nome do arquivo de núcleo variam, dependendo da plataforma:

- **AIX** **Linux** Um arquivo é criado normalmente, chamado `core`. Certifique-se de haver espaço suficiente no diretório do servidor para acomodar uma operação de dump. É comum ter um arquivo de dump com um tamanho de 2 GB para o servidor IBM Spectrum Protect de 32 bits. Além disso, certifique-se de que o `ulimit` para arquivos de núcleo esteja configurado como ilimitado para evitar que o arquivo de dump seja truncado.
- **Windows** O conteúdo do sistema é despejado automaticamente através de uma chamada da interface de programação de aplicativos de sistema (API). Se o servidor estiver em execução como um serviço, o arquivo de dump será chamado `dsmsvc.dmp`. Caso contrário, o arquivo dump será denominado `dsmserv.dmp`.

Se o sistema não foi configurado para capturar um arquivo de núcleo ou o sistema não tinha espaço suficiente para criar um arquivo de núcleo completo, ele pode ter seu uso limitado na determinação da causa do problema.

## Recuperando Arquivos da Biblioteca para Análise Principal

AIX

Linux

Arquivos principais são específicos do aplicativo, de bibliotecas e de outros recursos do sistema em uso pelo aplicativo no sistema onde ele estava em execução.

Para ler precisamente o arquivo principal em seu sistema de computador, todos os seguintes arquivos são necessários; eles estão localizados no diretório no qual o servidor está instalado:

- dsmserve
- dsmlicense
- ndmpsi
- dsmcored
- dsmaio
- centera

Os arquivos de biblioteca que são necessários variam entre todas as plataformas:

- **AIX** Colete os seguintes arquivos:
  - /usr/ccs/lib/libpthreads.a
  - /usr/ccs/lib/libc.a
  - Colete quaisquer outras bibliotecas carregadas, tais como saídas de mensagem. Para ver quais bibliotecas foram carregadas, chame dbx emitindo o comando **dbx dsmserve core\_file**. Em seguida, a partir do aviso do dbx, emita o comando **map** para mostrar todas as bibliotecas que estão carregadas e são necessárias para análise principal.
- **Linux** Emita o comando **ldd dsmserve** e envie em todas as bibliotecas compartilhadas dinâmicas. Por Exemplo:
  - libm.so.6 =>/lib64/libm.so.6
  - libnsl.so.1 =>/lib64/libnsl.so.1
  - libpthread.so.0 =>/lib64/libpthread.so.0
  - libdl.so.2 =>/lib64/libdl.so.2
  - libc.so.6 =>/lib64/libc.so.6
  - /lib64/ld64.so.1 =>/lib64/ld64.so.1

## Recuperando Arquivos de Log do Sistema

É possível recuperar arquivos de log do sistema para ajudá-lo a resolver as causas da interrupção do servidor.

Recupere os seguintes arquivos de log para fornecer ao serviço IBM:

- **AIX** Redirecione a saída do comando **errpt -a** em um arquivo: **errpt -a >errpt.txt**.
- **Linux** Copie o arquivo /var/log/messages.
- **Windows** Salve uma cópia de Logs de Evento, como visto no Event Viewer.

## Recuperando o Log de Atividades

Os arquivos de log de atividade podem ser recuperados para ajudar a resolver problemas com interrupções do servidor.

Visualize e colete entradas do log de atividades que começam pelo menos duas horas antes da interrupção e 30 minutos depois dela, emitindo o comando **QUERY ACTLOG**.

## Detectando Erros Após o Início e Parada do Serviço de Servidor

Windows

Se um serviço de servidor iniciar e parar inesperadamente, você poderá determinar a causa do erro solicitando um arquivo de log de erros.

### Sobre Esta Tarefa

Um serviço pode ser iniciado a partir do applet Serviços do Windows. Após iniciar o serviço, o serviço pode indicar que está iniciado, mas após ter sido atualizado, o serviço indica que está interrompido. Nas etapas a seguir, "Server1," é usado como o nome do servidor que foi iniciado e parado. Para determinar a causa do erro de Server1, conclua as seguintes etapas:

### Procedimento

1. Expanda **Tivoli Storage Manager > [Nome do Host] (Windows - Local) > Server1 > Relatórios > Informações de Serviço** para mostrar o serviço de servidor.
2. Na área de janela direita, clique com o botão direito do mouse no serviço **Server1** e selecione **Propriedades**.
3. Selecione a opção **Registrar Saída no Arquivo** e clique em **OK**.
4. Inicie o serviço Server1.
5. Se o serviço parar novamente, abra um editor de texto para ler o conteúdo do seguinte arquivo:  
C:\Program Files\Tivoli\TSM\Server1\console.log
6. Determine a causa do erro revisando as mensagens de erro que são geradas.

## O Diretório sqllib/db2dump Causa Encerramento

Os servidores Tivoli Storage Manager V6 podem encerrar inesperadamente se o diretório sqllib/db2dump for sobrecarregado. O momento mais comum para um encerramento é quando os arquivos First Occurrence Data Capture (FODC) do DB2 são gravados no diretório.

O diretório sqllib/db2dump é um caminho de diretório de dados diagnósticos que o DB2 usa para gravar informações de diagnóstico de FODC. Com o tempo, o DB2 pode gravar muitos arquivos FODC no diretório relacionado ao funcionamento do banco de dados. Quando arquivos não são removidos ou excluídos, o sistema de arquivos pode ficar cheio. O local dos arquivos First Occurrence Data Capture (FODC) do DB2 depende das suas definições de configuração do DB2 ou das configurações de variáveis ambientais do DB2.

Localize o diretório de dados diagnósticos verificando as definições de configuração do DB2 ou as configurações de variáveis de ambiente do DB2. Se os

arquivos no caminho de diretório de diagnóstico fizerem com que o sistema de arquivos fique cheio, efetue uma das seguintes ações:

- Inclua espaço no sistema de arquivos.
- Mova os arquivos para outro sistema de arquivos. Consulte o Tabela 6.
- Use o servidor para arquivar os arquivos e depois exclua-os usando as seguintes etapas:
  1. Execute o utilitário db2support para coletar as informações de diagnóstico do sistema DB2.
  2. Arquive o arquivo db2support.zip e arquivos de diagnóstico listados em Tabela 6 para o servidor com o clientet.
  3. Exclua os arquivos que estão listados no Tabela 6.

*Tabela 6. Arquivos que podem ser excluídos após estes arquivos serem arquivados*

Nome do arquivo	Descrição
instance_name.nfy instance_name.n.nfy (em que <i>n</i> é um número)	Logs de notificação de administração
db2dasdiag.log	Log de diagnóstico do DB2 Administration Server (DAS)
db2eventlog.xxx (em que <i>xxx</i> é o número da partição de banco de dados)	Log de eventos do DB2
nnnnnnn.nnnnn.nnn.dump.bin (em que <i>n</i> é um número)	Arquivos dump binários das estruturas na memória
nnnnnnn.n.nnn.trap.txt (em que <i>n</i> é um número)	Arquivos trap
nnnnnnn.nnnnn.nnn.apm.bin (em que <i>n</i> é um número)	Acesse os arquivos dump binários do gerenciador de planejamento
nnnnnnn.nnnnn.nnn.stack.txt (em que <i>n</i> é um número)	Rastreios de pilha
F0DC_xxxx/core<pid>	Arquivos principais  Estes diretórios F0DC_xxx contêm o registro de data e hora no nome de diretório. Mantenha os diretórios mais recentes e seus arquivos. O histórico pode ser útil para diagnosticar possíveis problemas futuros que estão relacionados ao banco de dados. Uma diretriz é mantê-los pelo menos por 1 semana.
events/db2optstats.n.log (em que <i>n</i> é um número)	Arquivo de Log de Estatísticas

**Dica:** Não exclua o arquivo db2diag.log e os arquivos no diretório stmmlog. O histórico que está contido neles pode ser útil para diagnosticar problemas do servidor que estão relacionados ao banco de dados.

#### **Referências relacionadas:**

“Localizando os Arquivos de Log de Diagnóstico do DB2” na página 79

## Resolvendo problemas com a verificação de página do banco de dados

A falha de validação de página durante o processamento de backup de banco de dados pode indicar dano no banco de dados, requerendo uma ação de reparo para corrigir o problema. Se a validação de página falhar, o backup de banco de dados também falhará.

### Procedimento

- Entre em contato com o suporte IBM para obter assistência no diagnóstico e reparo de qualquer dano no banco de dados.
- Se um backup de banco de dados completo estava em andamento para liberar espaço no diretório de log de archive, execute uma das seguintes ações:
  - Aumente a quantidade de espaço no diretório de log de archive.
  - Emita a opção ARCHFAILOVERLOGDIRECTORY para especificar um diretório de log de archive de failover no qual o servidor possa restaurar arquivos de log que não podem ser armazenados no diretório de log de archive.

Assegurar espaço adequado no diretório de log de archive permite que o servidor continue em execução enquanto o banco de dados é reparado.

---

## Resolvendo Erros do Banco de Dados

Os erros do banco de dados podem ser causados por problemas, como falta de espaço e por erros que são causados por operações de inserção, atualização ou exclusão.

Os usuários que são administradores experientes do DB2 podem executar consultas SQL avançadas e usar ferramentas do DB2 para monitorar o banco de dados, o espaço que está sendo usado e quaisquer erros. Quando estiver executando estas consultas, não use ferramentas do DB2 para alterar definições de configuração do DB2 das definições que são pré-configuradas pelo IBM Spectrum Protect ou não use nenhum outro software para modificar estas definições. O servidor deve ser usado com a linguagem de definição de dados e a configuração do banco de dados que o IBM Spectrum Protect implementa.

Para obter mais informações, consulte Informações do produto DB2.

## Resolvendo Problemas de Inicialização do Gerenciador de Banco de Dados

O servidor IBM Spectrum Protect pode não iniciar se o gerenciador do banco de dados DB2 estiver configurado para usar o plug-in dsmdb2pw. Quando o servidor não pode carregar o plug-in, o gerenciador de banco de dados não inicia e, por sua vez, o servidor falha ao iniciar.

Devido ao problema de plug-in, o servidor emite uma mensagem de erro semelhante a este exemplo:

```
db2start
SQL1365N db2start or db2stop failed in processing the plugin "dsmdb2pw".
Reason code = "10".
04/26/2011 16:04:11      0      0      SQL1365N
db2start or db2stop failed in processing the plugin "". Reason code = "".
```

Você também pode receber este erro:

```
SQL1032N No start database manager command was issued
```

Revise o arquivo db2diag.log para obter informações de diagnóstico relacionadas a esse tipo de erro.

Um exemplo de db2diag.log:

```
2011-04-26-16.04.11.820963-420 I2345542E1168          LEVEL: Error
PID      : 25178                      TID   : 47207843621184PROC : db2sysc 0
INSTANCE: hannigan NODE : 000
EDUID    : 1                        EDUNAME: db2sysc 0
FUNCTION: DB2 Common, OSSe, OSSHLibrary::load, probe:80
MESSAGE  : ECF=0x90000076=-1879048074=ECF_LIB_CANNOT_LOAD
          Cannot load the specified library
DATA #1 : Hex integer, 4 bytes
0x00000002
DATA #2 : String, 58 bytes
/home/hannigan/sql/lib/security64/plugin/server/dsmdb2pw.so
CALLSTCK:
[0] 0x00002AEF63DD267E pdOSSeLoggingCallback + 0x20C
[1] 0x00002AEF68486A42 /home/hannigan/sql/lib/lib64/libdb2osse.so.1 + 0x1C4A42
[2] 0x00002AEF6848825E ossLog + 0xA6
[3] 0x00002AEF684928E9 _ZN11OSSHLibrary4loadEPKcm + 0x1D3
[4] 0x00002AEF63F63BDC _Z20secLoadPluginGenericP19SEC_PLUGIN_HANDLE TPc + 0x68
[5] 0x00002AEF63F62FBB _Z23secLoadServerAuthPluginP19SEC_PLUGIN_HANDLE + 0x57
[6] 0x00002AEF63F6C833 _Z25sqllexLoadAllPluginsServerP5sqlca + 0x3B5
[7] 0x00002AEF6431737C /home/hannigan/sql/lib/lib64/libdb2e.so.1 + 0x123637C
[8] 0x00002AEF643164C5 sqloRunInstance + 0x191
[9] 0x00000000040D31D DB2main + 0xD41

2011-04-26-16.04.11.825930-420 I2346711E1178          LEVEL: Error
PID      : 25178                      TID   : 47207843621184PROC : db2sysc 0
INSTANCE: hannigan NODE : 000
EDUID    : 1                        EDUNAME: db2sysc 0
FUNCTION: DB2 Common, OSSe, OSSHLibrary::load, probe:90
MESSAGE  : ECF=0x90000076=-1879048074=ECF_LIB_CANNOT_LOAD
          Cannot load the specified library
DATA #1 : String, 109 bytes
../shared/gskit8/lib/linux64_x86/libgsk8iccs_64.so: cannot open shared object
file: No such file or directory
CALLSTCK:
[0] 0x00002AEF63DD267E pdOSSeLoggingCallback + 0x20C
[1] 0x00002AEF68486A42 /home/hannigan/sql/lib/lib64/libdb2osse.so.1 + 0x1C4A42
[2] 0x00002AEF6848825E ossLog + 0xA6
[3] 0x00002AEF6849294D _ZN11OSSHLibrary4loadEPKcm + 0x237
[4] 0x00002AEF63F63BDC _Z20secLoadPluginGenericP19SEC_PLUGIN_HANDLE TPc + 0x68
[5] 0x00002AEF63F62FBB _Z23secLoadServerAuthPluginP19SEC_PLUGIN_HANDLE + 0x57
[6] 0x00002AEF63F6C833 _Z25sqllexLoadAllPluginsServerP5sqlca + 0x3B5
[7] 0x00002AEF6431737C /home/hannigan/sql/lib/lib64/libdb2e.so.1 + 0x123637C
[8] 0x00002AEF643164C5 sqloRunInstance + 0x191
[9] 0x00000000040D31D DB2main + 0xD41
```

Na inicialização, o servidor detecta esses tipos de erros e tenta remover o plug-in da configuração. Se o servidor não puder remover o plug-in, você deverá removê-lo da configuração do gerenciador de banco de dados. Esse comando remove o plug-in da configuração do gerenciador de banco de dados:

```
db2 get database manager configuration | grep SRVCON_PW_PLUGIN
db2 update database manager configuration using SRVCON_PW_PLUGIN \"\"
```

## Rastreando o plug-in ID de usuário e senha

Se você configurar corretamente, o servidor poderá controlar automaticamente o plug-in ID de usuário e senha (dsmdb2pw).

Para configurar o rastreo automático para o plug-in ID de usuário e senha, conclua as seguintes etapas:

AIX

Linux

1. Certifique-se de que o servidor tenha autoridade de gravação para o diretório `~/sql1lib/db2dump/`.
2. Inclua o seguinte texto no arquivo `~instance/sql1lib/userprofile`:  
`export DB2_DS MDB2PW_TRACEFILE=filename`

em que *filename* é o caminho completo e o nome de arquivo do arquivo de rastreo, por exemplo `~/sql1lib/db2dump/dsmdb2pw.trc`.

3. Reiniciar o DB2

Depois da reinicialização do DB2, a saída de rastreo é armazenada no arquivo e diretório especificados.

Windows

1. Para verificar se o `DB2_VENDOR_INI db2set` está configurado, execute o comando `db2set`.
2. Se a variável `DB2_VENDOR_INI` não estiver configurada, crie um arquivo de configuração, por exemplo:  
`c:\Program Files\Tivoli\TSM\s1\tsmdbmgr.env`
3. Atualize o arquivo de configuração que está listado em `DB2_VENDOR_INI` com o local do arquivo de rastreo:  
`DB2_DS MDB2PW_TRACEFILE=c:\Program Files\Tivoli\TSM\s1\sql1lib\dsmdb2pw.trc`
4. Configure o arquivo de rastreo emitindo o seguinte comando:  
`db2set -i server_instance DB2_VENDOR_INI=configuration_file_location`

Por exemplo:

```
db2set -i s1 DB2_VENDOR_INI=c:\Program Files\Tivoli\TSM\s1\tsmdbmgr.env
```

5. Pare o servidor IBM Spectrum Protect e reinicie-o emitindo os comandos a seguir:  
`halt`  
`dsmserv -k server_instance`

Depois da reinicialização do servidor, a saída de rastreo é armazenada no arquivo e diretório especificados.

**Dica:** Você pode utilizar o nome de arquivo e o diretório de sua escolha para o nome e o local do arquivo de rastreo.

## Limitando a Alocação de Memória do DB2

Quando o DB2 usa uma grande quantidade de memória, é possível limitar a quantidade de memória usada pelo DB2, emitindo o comando **db2 update**.

### Sobre Esta Tarefa

Por padrão, o DB2 está instalado e configurado para usar o gerenciamento automático de memória, que faz com que o DB2 use uma grande porcentagem de memória física. Para restringir a quantidade de memória, use o comando **db2 update** para especificar o limite de memória.

### Procedimento

Emita o comando **db2 update**:

```
db2 update dbm cfg using instance_memory memory_value
```

em que *memory\_value* é especificado em blocos de 4 KB.

### Exemplo

Para limitar a alocação de memória do DB2 para usar 3.200.000 KB de memória, divida 3.200.000 KB em blocos de 4 KB, que produz um resultado de 800000. Em seguida, emita o seguinte comando:

```
db2 update dbm cfg using instance_memory 800000
```

Para obter mais informações sobre a configuração de memória da instância, consulte o Informações do produto DB2.

## Recuperando Informações da Versão do DB2

A versão do DB2 que está instalada com o servidor IBM Spectrum Protect é periodicamente atualizada. Se ocorrerem problemas do banco de dados, você deverá saber a versão do DB2 e seu local para que seja possível fornecer estas informações para o Suporte de Software IBM.

### Procedimento

Emita o comando **db2level** para mostrar onde os produtos DB2 estão instalados em seu servidor e para listar o nível do produto DB2.

A saída a seguir mostra os resultados de amostra do comando **db2level**.

AIX

Linux

```
> db2level
DB21085I This instance or install (instance name, where applicable:
"cetinst1") uses "64" bits and DB2 code release "SQL10051" with level
identifier "0602010E".
Informational tokens are "DB2 v10.5.0.1", "special_31150",
"IP23526_31150", and Fix Pack "1".
Product is installed at "/opt/tivoli/tsm/db2".
```

Windows

```
C:\>db2level
DB21085I This instance or install (instance name, where applicable: "SERVER1")
uses "64" bits and DB2 code release "SQL10051" with level identifier
"0602010E".
Informational tokens are "DB2 v10.5.100.64", "special_31150",
"IP23521_31155", and Fix Pack "1".
Product is installed at "C:\PROGRA~1\Tivoli\TSM\db2" with DB2 Copy Name "DB2TSM1".
```



## Localizando os Arquivos de Log de Diagnóstico do DB2

O arquivo `db2diag.log` contém informações de diagnóstico que podem ajudá-lo a resolver problemas que possam ocorrer com seus bancos de dados.

O local do arquivo `db2diag.log` e os arquivos DB2 first occurrence data capture (FODC) dependem das suas definições de configuração DB2 ou configurações de variável ambiental DB2. O DB2 grava mensagens sobre operações internas, eventos ou status no arquivo de log de notificação de administração (`db2SID.nfy`).

AIX

Linux

Conclua as seguintes etapas para determinar onde o caminho do diretório de dados diagnósticos está localizado:

1. Efetue login como a instância do usuário do servidor.
2. Emita o seguinte comando:

```
db2 get dbm cfg | grep DIAGPATH
```

Se nenhum caminho estiver especificado no parâmetro de configuração **DIAGPATH**, o diretório de dados diagnósticos estará no subdiretório `sqliib/db2dump` do diretório de instâncias. Por exemplo, `/home/tsminst1/sqliib/db2dump`, em que `/home/tsminst1` é o diretório inicial da instância.

Windows

Conclua as seguintes etapas para determinar onde o caminho do diretório de dados diagnósticos está localizado:

1. Pare o modo interativo do DB2. Inicie um prompt de linha de comandos do DB2 e emita o comando `quit`.
2. Localize o caminho usando o parâmetro de configuração **DIAGPATH**. Emita o comando

```
db2 get dbm cfg | findstr /s /i diagpath
```

3. Se nenhum caminho estiver especificado no parâmetro de configuração **DIAGPATH**, o caminho do diretório `DB2INSTPROF` será usado. Localize o caminho que foi configurado na variável de ambiente `DB2INSTPROF`. Emita o seguinte comando a partir do prompt de linha de comandos do DB2:

```
db2set db2instprof
```

A saída deste comando mostra o local dos arquivos de dados DB2. O arquivo de log de diagnóstico no subdiretório de instância do diretório que é especificado pela variável de registro `DB2INSTPROF`. Por exemplo, para a instância de servidor `TSMSEVER1`, o comando **db2set db2instprof** mostra este caminho:

```
C:\ProgramData\IBM\DB2\DB2TSM1
```

O arquivo de log de diagnóstico está no subdiretório `TSMSEVER1`:

```
C:\ProgramData\IBM\DB2\DB2TSM1\TSMSEVER1
```

4. Se a variável de ambiente `DB2INSTPROF` não estiver configurada, `x:\Sqliib\DB2INSTANCE` será usado. `x:\Sqliib` é a referência da unidade e também é o diretório que é especificado na variável de registro `DB2PATH`. O valor de `DB2INSTANCE` é o nome da instância. Não é necessário chamar o diretório `Sqliib`. A primeira parte da saída do comando **db2set db2path** é o caminho do diretório de dados diagnósticos com o nome de instância incluído. A saída mostra o caminho do diretório a seguir:

```
C:\Program Files\Tivoli\TSM\db2\TSMINST1
```

em que *DB2PATH* é C:\Program Files\Tivoli\TSM\db2 e o nome da instância é TSMINST1.

**Referências relacionadas:**

“Arquivos de Log de Instalação” na página 64

## Arquivos de Log de Upgrade do DB2

Ao fazer upgrade do servidor IBM Spectrum Protect, o script **db2ckupgrade** do DB2 é executado e cria arquivos de log para os bancos de dados do servidor.

Durante o upgrade, o assistente corrige automaticamente alguns erros no banco de dados. Você deve corrigir outros erros manualmente. Verifique nos arquivos de log os erros que devem ser corrigidos. Os arquivos de log contêm os resultados do comando **db2ckupgrade** para cada banco de dados.

Os seguintes arquivos de log são criados durante um upgrade:

- **AIX** **Linux** /tmp/db2ckupgrade\_instance\_name\_db\_name.log
- **Windows** installation\_directory\db2ckupgrade\_instance\_name\_db\_name.log

Se receber uma mensagem de erro do banco de dados quando o script estiver executando o que o assistente não corrigir, você deverá cancelar ou fechar o assistente, corrigir o erro e iniciar o upgrade novamente. Se for uma instalação silenciosa que está sendo concluída, você deverá verificar erros no arquivo log.text, corrigir os erros neste arquivo e iniciar o upgrade novamente. Para obter detalhes sobre mensagens de erro listadas nos arquivos de log, consulte o Informações do produto DB2.

## Resolvendo um Problema de ID do Banco de Dados Ausente ou Incorreto

Se você restaurar um banco de dados para um servidor diferente após um desastre, o arquivo de ID do banco de dados (dsmserv.dbid) poderá não ser restaurado. O servidor IBM Spectrum Protect, portanto, não pode localizar o arquivo após a operação de restauração e não pode ser iniciado.

Após fazer upgrade do Tivoli Storage Manager versão 6.1 para 6.2, você poderá ter dificuldade para restaurar os bancos de dados do Tivoli Storage Manager V6.1. Deve-se iniciar o servidor Tivoli Storage Manager V6.2 para gerar uma nova imagem de backup no DB2. Após a inicialização do servidor Tivoli Storage Manager V6.2, um backup de banco de dados será iniciado automaticamente. Quando o backup for concluído, pare o servidor e emita o comando **RESTORE DB**. Se o backup automático do banco de dados não for concluído com êxito, resolva o problema e emita o comando **BACKUP DB**. Assegure-se de que ele seja concluído antes de emitir o comando **RESTORE DB**.

**Importante:** Deve-se ter uma imagem de backup do banco de dados bem-sucedida gerada pelo servidor Tivoli Storage Manager V6.2 para que backups de banco de dados incremental ou restaurações de banco de dados sejam bem-sucedidos.

Se você iniciou o servidor Tivoli Storage Manager V6.2 transferido por upgrade e o backup do banco de dados automático foi concluído com sucesso, será possível descartar o banco de dados antes de restaurá-lo. Não se deve eliminar o banco de dados imediatamente após o upgrade para a V6.2. Se você descartar o banco de dados antes que uma imagem de backup seja gerada, deverá reinstalar o servidor Tivoli Storage Manager V6.1 e, em seguida, restaurar o banco de dados.

Se for necessário restaurar um banco de dados Tivoli Storage Manager V6.1 e o banco de dados não existir, deve-se fazê-lo por meio do Tivoli Storage Manager V6.1. Em seguida, será possível fazer upgrade para o Tivoli Storage Manager V6.2.

Um arquivo dbid perdido ou incorreto pode afetar o início do servidor após uma operação de restauração do banco de dados.

Quando um banco de dados for restaurado, o arquivo de ID do banco de dados deverá permanecer sincronizado com o banco de dados. Com o Tivoli Storage Manager V6.2, se você formatar o banco de dados antes de restaurá-lo, o arquivo de ID do banco de dados será mudado. Esta mudança causa uma incompatibilidade da data e hora no banco de dados e impede que o servidor seja iniciado.

Se o arquivo de ID do banco de dados estiver causando erros durante uma operação de restauração, você poderá ter de usar o parâmetro -S (ignorar verificação de ID do BD). O arquivo dsmserv.dbid deve estar ausente do servidor ao usar o parâmetro -S. As seguintes situações descrevem onde o parâmetro -S é útil:

- Se você reformatar o servidor após seu backup, terá uma incompatibilidade da data e hora armazenada no novo arquivo dsmserv.dbid. Use o parâmetro -S quando iniciar o servidor após a restauração.
- Quando o arquivo dsmserv.dbid for danificado ou perdido.

Após o uso inicial do parâmetro -S em um cenário de restauração, o servidor criará um arquivo dsmserv.dbid no diretório de instâncias.

## Resolvendo Problemas com os Comandos BACKUP DB e RESTORE DB

Os comandos **BACKUP DB** e **RESTORE DB** do servidor solicitam que o aplicativo de banco de dados IBM DB2 faça backup do banco de dados IBM Spectrum Protect para o servidor.

Os dados de backup são então enviados para o servidor usando a interface de programação de aplicativo (API) do cliente.

Quando um comando **BACKUP DB** ou **RESTORE DB** falha com uma mensagem DB2 SQLCODE ou SQLERRMC com códigos de retorno, obtenha uma descrição do DB2 SQLCODE executando os seguintes procedimentos:

1. Abra uma interface de linha de comandos do DB2:

**Windows** No Windows, clique em **Iniciar > Todos os Programas > IBM DB2** e clique em **Ferramentas de Linha de Comandos > Processador de Linha de Comandos**.

**AIX** **Linux** Para todas as demais plataformas suportadas, efetue logon no ID da instância do DB2 e abra uma janela de shell; em seguida, emita o comando DB2.

2. Insira o SQLCODE. Por exemplo, se o DB2 SQLCODE for -2033, emita o seguinte comando:  
? sql2033

É possível usar os detalhes da condição de erro para depurar o problema com o comando **BACKUP DB** ou **RESTORE DB**. Se o código SQLERRMC também for exibido,

ele será explicado na descrição SQLCODE fornecida. É possível localizar informações adicionais sobre os códigos de retorno da API através dos seguintes arquivos:

- **Windows** tsm\api\include\dsmrc.h
- **AIX** **Linux** tsm/client/api/bin64/sample/dsmrc.h

## Resolvendo Variáveis de Ambiente Incorretas para BACKUP DB e RESTORE DB

Muitos dos problemas de processamento **BACKUP DB** ou **RESTORE DB** são um resultado de conjunto incorreto de variáveis de ambiente DSMI\_CONFIG, DSMI\_DIR ou DSMI\_LOG.

### Sobre Esta Tarefa

#### Requisito:

As variáveis de ambiente são usadas pela API do cliente para localizar códigos de API e os arquivos de opções. A instância do DB2 deve estar em execução em um shell com variáveis de ambiente configuradas corretamente.

**AIX** **Linux** As variáveis DSMI\_\* estão configuradas no arquivo userprofile da instância. Por exemplo: /home/tsminst1/sql1lib/userprofile

**Windows** As variáveis DSMI\_\* estão configuradas no arquivo para o qual a variável de registro de instância do DB2, DB2\_VENDOR\_INI, aponta. Por exemplo, esse arquivo pode ser c:\tsminst1\tsmdbmgr.env. Você pode verificar o nome do arquivo e o local emitindo o comando db2set -i tsminst1 DB2\_VENDOR\_INI, em que tsminst1 é a instância do DB2.

As variáveis DSMI\_\* são inicialmente configuradas automaticamente pelo assistente de configuração de instância do IBM Spectrum Protect.

### Procedimento

Abra o arquivo /home/tsminst1/sql1lib/userprofile e revise as instruções. Se você alterar esse arquivo, pare e reinicie a instância do DB2 para que as mudanças sejam incluídas. Por exemplo, considere o seguinte cenário. O arquivo userprofile tem instruções como o seguinte texto de exemplo:

```
export DSMI_CONFIG=server_instance_directory/tsmdbmgr.opt
export DSMI_DIR=server_bin_directory/dbbkapi
export DSMI_LOG=server_instance_directory
```

O arquivo tsmdbmgr.opt possui o texto a seguir:

```
SERVERNAME TSMDBMGR_TSMINST1
```

O arquivo server\_bin\_directory/dbbkapi/dsm.sys possui o texto a seguir:

```
SERVERNAME TSMDBMGR_TSMINST1
commethod tcpip
tcpserveraddr localhost
errorlogname /tsminst1/tsmdbmgr.log
```

Verifique se a entrada SERVERNAME no arquivo tsmdbmgr.opt corresponde à entrada SERVERNAME no arquivo dsm.sys.


**Linux** Não inclua a opção de geração PASSWORDACCESS no arquivo de configuração dsm.sys. Esta opção pode causar falha do backup de banco de dados.

## Resolvendo a Mensagem de Erro ANR2968E

A mensagem de erro ANR2968E é exibida durante o comando **BACKUP DB**.

### Sobre Esta Tarefa

Existem duas causas para esta mensagem de erro:

- Se o arquivo de log de erros do IBM Spectrum Protect for de propriedade do ID do usuário root e não do ID do usuário da instância de servidor.
-  Se você usar aspas entre os caminhos que estão no arquivo `tsmdbmgr.env`. Use um caminho que não contenha espaços ou use o nome abreviado do Windows para o caminho.

Para corrigir o erro causado pelo ID do usuário root, conclua as seguintes etapas:

### Procedimento

1. Efetue login usando um ID da instância do servidor IBM Spectrum Protect e verifique o nome do arquivo de log de erro. Por exemplo:

```
$ grep -i "ERRORLOGNAME" $DSMI_DIR/dsm.sys
ERRORLOGNAME /home/db2inst1/tsminst1/tsmdbmgr.log
```

em que `db2inst1` é o ID do usuário da instância de servidor e `/home/db2inst1/tsminst1/` é o diretório da instância de servidor.

2. Emita o seguinte comando de exemplo para verificar o proprietário atual do arquivo de log de erros:

```
$ ls -la /home/db2inst1/tsminst1/tsmdbmgr.log
-rw-r--r-- 1 root system 834 May 05 09:43 /home/db2inst1/tsminst1/tsmdbmgr.log
```

3. Se o arquivo de log de erros não for de propriedade do ID do usuário da instância do IBM Spectrum Protect, remova-o. Você deve ter autoridade de administrador para remover o arquivo. Emita o seguinte comando de exemplo para o arquivo de log:

```
$ su root password
# rm /home/db2inst1/tsminst1/tsmdbmgr.log
# exit
```

4. Emita o comando **BACKUP DB** e verifique se o comando foi concluído com êxito. Verifique se o arquivo de log é de propriedade do ID da instância de servidor. Por exemplo:

```
$ ls -la /home/db2inst1/tsminst1/tsmdbmgr.log
-rw-r--r-- 1 db2inst1 db2iadml 834 May 05 09:50
/home/db2inst1/tsminst1/tsmdbmgr.log
```

## Resolvendo Problemas da Mensagem de Erro ANR2971E Usando o Código SQL

A mensagem de erro ANR2971E pode ser mostrada quando você restaura ou efetua backup de uma operação do banco de dados e o processo para. Use o código SQL anexado ao erro para ajudá-lo a resolver o problema.

### Antes de Iniciar

Se você estiver restaurando um banco de dados porque o servidor foi interrompido durante operação normal, revise o arquivo `db2diag.log` antes de fazer backup ou restaurar o banco de dados.

A mensagem a seguir pode ser emitida durante a restauração ou o backup de dados:

ANR2971E Backup/restaur./rollforward do BD encerrados - DB2 sqlcode - erro 2581

No cenário a seguir, o processo **DSMSERV RESTORE DB** falhou com um código DB2 SQL 2581. O cenário a seguir não pertence aos problemas com as variáveis de ambiente DSMI.

## Procedimento

1. Emita o seguinte comando a partir da interface da linha de comandos do DB2:  
? SQL2581

É gerada uma explicação sobre o código SQL.

SQL2581N A restauração não pode extrair arquivos de log ou restaurar um diretório de log da imagem de backup para o caminho especificado.  
Código de razão 2581

2. Revise o arquivo db2diag.log no qual é possível localizar mensagens de status e de erro. Uma parte do arquivo db2diag.log é exibida no seguinte exemplo:

```
2009-02-10-09.49.00.660000-300 E8120712F500      LEVEL: Informativo
PID      : 4608                      TID   : 3956      PROC  : db2syscs.exe
INSTANCE: SERVER1                   NODE  : 000      DB   : TSMDB1
APPHDL   : 0-7                      APPID: *LOCAL.SERVER1.090210144859
AUTHID   : B1JRP01
EDUID    : 3956                      EDUNAME: db2agent (TSMDB1)
FUNCTION: DB2 UDB, utilitários de banco de dados, sqludPrintStartingMsg,
análise:1292
DATA #1 : <preformatted>
Iniciando uma restauração do banco de dados completa.
IDE de EDU do Agente: 3956
```

```
2009-02-10-09.50.21.051000-300 E8123213F483      LEVEL: Grave
PID      : 4608                      TID   : 5080      PROC  : db2syscs.exe
INSTANCE: SERVER1                   NODE  : 000
EDUID    : 5080                      EDUNAME: db2bm.3956.1 (TSMDB1)
FUNCTION: DB2 UDB, utilitários de banco de dados, sqluWriteLogFile,
análise:1498
MESSAGE  : ZRC=0x850F000C=-2062614516=SQL0_DISK "Disco cheio."
          DIA8312C O disco estava cheio.
DATA #1 : Cadeia, 46 bytes
F:\tivoli\tsm\Beta\sarch\RstDbLog\S0000262.LOG
```

```
2009-02-10-09.50.21.051000-300 E8124165F912      LEVEL: Grave
PID      : 4608                      TID   : 5080      PROC  : db2syscs.exe
INSTANCE: SERVER1                   NODE  : 000
EDUID    : 5080                      EDUNAME: db2bm.3956.1 (TSMDB1)
FUNCTION: DB2 UDB, utilitários de banco de dados, sqluWriteLogFile,
análise:1500
MESSAGE  : SQL2581N Não foi possível para restauração extrair arq de log
          ou restaurar um dir de log da imagem de backup para o
          caminho especificado. Código razão "".
DATA #1 : SQLCA, PD_DB2_TYPE_SQLCA, 136 bytes
sqlcaid : SQLCA      sqlcabc: 136      sqlcode: -2581      sqlerrml: 1
sqlerrmc: 4
sqlerrp : sqluWrit
sqlerrd : (1) 0x00000000      (2) 0x00000000      (3) 0x00000000
          (4) 0x00000000      (5) 0x00000000      (6) 0x00000000
sqlwarn : (1)      (2)      (3)      (4)      (5)      (6)
          (7)      (8)      (9)      (10)     (11)
sqlstate:
```

O exemplo anterior mostra pela mensagem “Disco Cheio” que não havia espaço suficiente em disco para colocar os arquivos de log necessários da operação de backup.

3. Inclua espaço em disco e execute novamente a operação.

## Erros Comuns de BACKUP DB e RESTORE DB

Os erros comuns derivados dos comandos **BACKUP DB** ou **RESTORE DB** podem incluir códigos de retorno ou de erro SQL.

Os erros a seguir são alguns dos erros mais comuns exibidos durante a emissão dos comandos **BACKUP DB** ou **RESTORE DB**.

### **ANR2968E - Backup de banco de dados terminado DB2 SQLCODE -2033 SQLERRMC 406**

Para resolver a mensagem de erro SQL 406, certifique-se de que os seguintes problemas tenham sido resolvidos:

- A variável de ambiente `DSMI_CONFIG` aponta para um arquivo de opções do IBM Spectrum Protect válido.
- O proprietário da instância tem acesso de leitura ao arquivo `dsm.opt`.
- A variável de ambiente `DSMI_CONFIG` está configurada em `~/sqllib/userprofile` e `~/sqllib/usercshrc`.

### **DB2 SQLCODE: -2033, DB2 SQLERRMC: 106**

Se você receber a mensagem de erro SQL 106, isso pode significar que há um problema de permissões com o arquivo de log na qual a interface de programação de aplicativos (API) do cliente grava.

Para resolver o erro, localize o arquivo de log com o problema de permissões, efetue login usando o ID do usuário root e exclua o arquivo.

### **DB2 SQLCODE: -2033, DB2 SQLERRMC: 168**

Verifique se a variável de ambiente `DSMI_DIR` aponta para o diretório executável da API do cliente que contém o agente de comunicação confiável `dsmtca`.

### **ANR2971E - Backup/Restauração/Rollforward do Banco de Dados Finalizados DB2 SQLCODE - Erro 2071**

A biblioteca não pode ser carregada porque a biblioteca ou uma biblioteca requerida por esta biblioteca não existe ou não possui um formato válido. Se uma biblioteca não puder ser carregada, isso significa que uma biblioteca de 32 bits está sendo carregada em uma instância de 64 bits, ou uma biblioteca de 64 bits está sendo carregada em uma instância de 32 bits. Se uma biblioteca não puder ser carregada, isso também indica que a variável de ambiente `DSMI_DIR` aponta para os arquivos executáveis incorretos da API do cliente IBM Spectrum Protect. Para obter informações sobre o erro, abra uma janela do processador de linha de comandos do DB2 e emita o seguinte comando:

```
db2 => ? sql2071
```

Verifique se alguma mudança foi feita nos arquivos `tsmdbmgr.opt`, `dsm.sys` ou `sqllib/userprofile`; a instância do DB2 é reciclada para selecionar os novos valores. Para reciclar a instância do DB2, pare e inicie o servidor IBM Spectrum Protect. Além disso, verifique se o comando **EXPORT** precede as entradas `DSMI_*` no arquivo `sqllib/userprofile`.

## Mensagem de Erro Indica que o Nó Está Bloqueado

Você pode receber um erro quando o DB2 entra em contato com o servidor e um nó específico e recebe uma mensagem de erro que indica que o nó está bloqueado.

Para corrigir o erro, use o endereço do host local em vez de um endereço de loopback explícito, por exemplo, 127.0.0.1. Especifique a opção `tcpserveraddress localhost` na sub-rotina `SERVERNAME TSMDBMGR_TSMINST1` do arquivo `dsm.sys`.

## Problemas com o Desempenho do Backup de Banco de Dados

Em alguns casos, especificamente em sistemas AIX, se o servidor estiver configurado para usar TCP/IP para operações de backup e restauração do banco de dados, os backups de banco de dados podem ficar lentos. Para resolver o problema, configure a instância do servidor para usar memória compartilhada.

### Tarefas relacionadas:

“Configurando uma Instância do Servidor para Usar Memória Compartilhada” na página 60

## Características do ID do Usuário `$$_TSMDBMGR_$$`

O servidor IBM Spectrum Protect gera o ID do usuário `$$_TSMDBMGR_$$` na inicialização.

Você pode visualizar o ID do usuário `$$_TSMDBMGR_$$` nos resultados de um comando **QUERY SESSION**. Esse ID também é apresentado no arquivo de log de atividade e em outros arquivos de log do servidor.

O servidor usa o ID de usuário `$$_TSMDBMGR_$$` para fazer backup do banco de dados do servidor. Usando o ID do usuário `$$_TSMDBMGR_$$`, você pode tornar o banco de dados acessível para processamento caso o servidor esteja indisponível. A mudança desse ID coloca em risco a capacidade de recuperação ou restauração de um servidor no caso de desastre.

**Restrição:** Você não pode alterar o arquivo `dsm.sys` ou `dsm.opt` para configurar ou usar um nome de nó cliente diferente. O banco de dados do servidor IBM Spectrum Protect local usa o arquivo `dsm.sys` ou `dsm.opt` para efetuar backup de seu próprio banco de dados.

## Resolvendo Problemas de Reorganização de Banco de Dados

A reorganização de tabelas de banco de dados e de índices exige uma quantidade significativa de recursos do sistema. Para evitar a ocupação de recursos do sistema que podem ser usados de outra forma, execute suas rotinas de reorganização em horários de inatividade.

O crescimento inesperado do banco de dados e os requisitos inesperados de espaço de log de archive e ativo podem ocorrer se as tabelas ou os índices associados às tabelas não forem reorganizados. O IBM Spectrum Protect reorganiza as tabelas por padrão. Se a reorganização automática estiver afetando o desempenho do servidor, você poderá planejar a reorganização manualmente.

As seguintes sugestões podem ajudá-lo a configurar sua reorganização:

- Ative a reorganização de índice se estiver executando a deduplicação em seu servidor. Consulte a opção do servidor `ALLOWREORGINDEX`.



- Por padrão, a reorganização de tabela fica ativada 24 horas por dia. Execute a reorganização durante um tempo relativamente inativo durante o dia. Consulte as seguintes opções do servidor para definir um tempo inativo quando a reorganização puder executar:
  - REORGBEGINTIME
  - REORGDURATION

---

## Analizando os Sintomas do Processo para Resolver Problemas

Às vezes é possível determinar a causa dos erros observando os sintomas do processo.

É possível encontrar um dos seguintes sintomas do processo:

- Espaço insuficiente em um conjunto de armazenamentos de cópia de destino
- Localizado arquivo danificado no volume
- Os arquivos não expiram após a redução do número de versões que precisam ser mantidas
- A Migração Não É Executada para o Conjunto de Armazenamentos de Mídia Sequencial
- A migração usa apenas um processo
- Execução lenta do processo

## Revisando as Mensagens do Processo para Determinar o Estado de Operações do Servidor

Os processos do servidor, se executados em primeiro plano ou em segundo plano, sempre emitirão uma mensagem “processo iniciado” e uma mensagem “processo terminado”, além das mensagens de processo gerais. É possível usar estas mensagens para determinar o status de sua operação do servidor.

### Processos executados no servidor

Um processo do servidor é uma tarefa executada no servidor. É possível designar a tarefa para executar uma operação específica, como migração de dados de um conjunto de armazenamentos para o próximo conjunto de armazenamentos na hierarquia. Emita os processos do servidor para resolver problemas com seu servidor.

Os processos do servidor normalmente são iniciados como um processo automatizado no servidor. O processo poderá ou não ser influenciado por uma opção do servidor ou por outra configuração. O processo do servidor também pode ser iniciado por um comando.

Muitos processos do servidor podem ser executados no PRIMEIRO PLANO ou de forma síncrona. Os processos executados no PRIMEIRO PLANO podem ser iniciados por um comando usando o parâmetro WAIT=YES. Os comandos que iniciam processos do servidor que não permitem o parâmetro WAIT=YES ou os comandos especificados com WAIT=NO são executados no SEGUNDO PLANO ou de forma assíncrona.

Alguns processos do servidor podem iniciar vários processos simultaneamente para executar a tarefa. Consulte a Tabela 7 na página 88 para obter as descrições dos processos do servidor.

Tabela 7. Processos do Servidor

Processo ou comando	descrição	É executado no primeiro plano ou como um processo múltiplo
<b>AUDIT VOLUME</b>	Faz auditoria do conteúdo de um volume para validar se os dados ainda podem ser lidos e se as definições do banco de dados do servidor que descrevem os dados estão corretas.	
<b>BACKUP DB</b>	Faz backup do banco de dados do servidor (COMPLETO ou INCREMENTAL).	O <b>BACKUP DB</b> pode ser executado como um processo síncrono especificando <b>WAIT=YES</b> .
<b>BACKUP STGPOOL</b>	Faça backup de um conjunto de armazenamento do servidor principal para um conjunto de armazenamento de cópia. O resultado é que você pode fazer cópias duplicadas dos dados e potencialmente obter cópias duplicadas em um local externo.	O <b>BACKUP STGPOOL</b> pode ser executado como um processo síncrono especificando <b>WAIT=YES</b> . <b>BACKUP STGPOOL</b> pode ser executado usando vários processos simultâneos, o que é controlado pelo parâmetro <b>MAXPROCESS</b> especificado no comando <b>BACKUP STGPOOL</b> .
<b>CHECKIN LIBVOLUME</b>	Verifica um volume da fita em uma biblioteca de fitas.	
<b>CHECKOUT LIBVOLUME</b>	Verifica um volume da fita fora de uma biblioteca de fitas.	
<b>Expiration</b>	<p>Exclua arquivos de backup e archive do cliente do servidor, com base nas políticas definidas para gerenciar esses arquivos.</p> <p>É possível executar a expiração automaticamente, especificando <b>EXPINTERVAL=<i>n</i></b> no arquivo de opções do servidor, em que <i>n</i> é qualquer número diferente de zero. A expiração também pode ser iniciada emitindo o comando <b>EXPIRE INVENTORY</b>. Não é possível ter mais de um processo de expiração em execução por vez, embora seja possível executar mais de um encadeamento por vez.</p>	O comando <b>EXPIRATION</b> pode ser executado como um processo síncrono especificando <b>WAIT=YES</b> .

Tabela 7. Processos do Servidor (continuação)

Processo ou comando	descrição	É executado no primeiro plano ou como um processo múltiplo
<b>IMPORT</b>	<p>Importa dados de volumes de mídia sequencial ou diretamente de outro servidor usando conexões de comunicação TCP/IP entre os servidores.</p> <p>O processamento de importação pode ser iniciado por qualquer um dos seguintes comandos:</p> <ul style="list-style-type: none"> <li>• <b>IMPORT ADMIN</b></li> <li>• <b>IMPORT NODE</b></li> <li>• <b>IMPORT POLICY</b></li> <li>• <b>IMPORT SERVER</b></li> </ul>	
<b>LABEL LIBVOLUME</b>	Rotula um ou mais volumes de biblioteca em uma biblioteca.	
<b>Migração</b>	<p>Migra dados de um conjunto de armazenamentos para o próximo na hierarquia de armazenamento.</p> <p>A migração é iniciada e parada, com base nos limites HighMig e LowMig definidos para o conjunto de armazenamentos. Sempre que <b>UPDATE STGPOOL</b> for emitido, estes valores serão reexaminados e, se apropriado, <b>MIGRATION</b> é iniciado. Caso contrário, o servidor monitorará a porcentagem de utilização para dados não migrados em um conjunto de armazenamento. Conforme a necessidade do servidor, ele inicia o processamento de migração para esse conjunto de armazenamento quando o limite HighMig é excedido. Também é possível emitir o comando <b>MIGRATE STGPOOL</b> para iniciar o processamento de migração manualmente.</p>	A migração pode ser configurada para executar vários processos simultâneos. Os vários processos são controlados pelo atributo MIGPROCESS do conjunto de armazenamento e pode ser atualizado emitindo o comando <b>UPDATE STGPOOL</b> .
<b>MOVE DATA</b>	Move dados de um volume para outros volumes no mesmo conjunto de armazenamentos ou para um conjunto de armazenamentos diferente.	O comando <b>MOVE DATA</b> pode ser executado como um processo síncrono especificando WAIT=YES.
<b>MOVE DRMEDIA</b>	Gerencia a mídia de recuperação de desastre movendo volumes no site para fora do site ou retornando volumes externos no site. A mídia de recuperação de desastres são os volumes de backup de banco de dados e de backup do conjunto de armazenamentos necessários para proteger e recuperar o servidor.	O comando <b>MOVE DRMEDIA</b> pode ser executado como um processo síncrono especificando WAIT=YES.

Tabela 7. Processos do Servidor (continuação)

Processo ou comando	descrição	É executado no primeiro plano ou como um processo múltiplo
<b>MOVE MEDIA</b>	Move volumes de uma biblioteca de fitas para o local para excesso para evitar que uma biblioteca fique cheia.	
<b>MOVE NODEDATA</b>	Move todos os dados para o nó ou nós especificados para outros volumes no mesmo conjunto de armazenamentos ou para um conjunto de armazenamentos diferente.	O comando <b>MOVE NODEDATA</b> pode ser executado como um processo síncrono especificando WAIT=YES.
<b>PREPARE</b>	Cria um arquivo de plano de recuperação.	O comando <b>PREPARE</b> pode ser executado como processo síncrono especificando WAIT=YES.
<b>Reclamação</b>	<p>Recupera espaço de volumes da fita movendo dados ativos para outros volumes e retornando o volume para vazio e privado, ou então para o início.</p> <p>O servidor monitora o <b>RECLAMATION THRESHOLD</b> definido para um conjunto de armazenamentos. Ele inicia um processo de recuperação para esse conjunto de armazenamentos para recuperar os volumes elegíveis, se determinar que existem um ou mais volumes elegíveis.</p>	
<b>RESTORE STGPOOL</b>	Restaura todos os arquivos para um determinado conjunto de armazenamentos a partir de um conjunto de armazenamentos de cópia.	O <b>RESTORE STGPOOL</b> pode ser executado como um processo síncrono especificando WAIT=YES. <b>RESTORE STGPOOL</b> pode ser executado usando vários processos simultâneos, o que é controlado pelo parâmetro <b>MAXPROCESS</b> especificado no comando <b>RESTORE STGPOOL</b> .
<b>RESTORE VOLUME</b>	Restaura todos os arquivos para um determinado volume a partir de um conjunto de armazenamentos de cópia.	O comando <b>RESTORE VOLUME</b> pode ser executado como um processo síncrono especificando WAIT=YES. <b>RESTORE VOLUME</b> pode ser executado usando vários processos simultâneos, o que é controlado pelo parâmetro <b>MAXPROCESS</b> especificado no comando <b>RESTORE VOLUME</b> .

## Mensagens emitidas quando os processos são iniciados

Quando o servidor executa tarefas como processos, uma mensagem de identificação e um relatório de que os processos foram iniciados são designados a eles.

O início relatado é emitido na seguinte mensagem:

ANR0984I Processo *process\_id* para *process\_name* iniciado no *process\_state* às *time*

A lista a seguir define as variáveis a partir desta mensagem:

*process\_id*

Identificador de processo numérico.

*process\_name*

O nome do processo.

*process\_state*

**FOREGROUND** ou **BACKGROUND**. Se o processo estiver em execução no primeiro plano, isto indica que o comando foi emitido com o parâmetro **WAIT=YES**. O processamento em primeiro plano faz a sessão administrativa que emitiu o comando aguardar até a conclusão do processamento. Um processo em execução no segundo plano retorna imediatamente à sessão administrativa que emitiu o comando, indicando que um processo foi iniciado enquanto o processo ainda está em execução. Os processos em execução no segundo plano podem ser monitorados com o comando **QUERY PROCESS**.

*time* O horário de início do processo.

## Mensagens emitidas quando os processos são terminados

Quando o servidor executa tarefas como processos, os processos são relatados quando terminam. As mensagens “processo terminado” que são emitidas variam de processo para processo. A mensagem depende se o processo precisa relatar itens e bytes processados, nenhum item ou byte processado, itens processados ou apenas bytes processados.

### Processo Terminado

Quando um processo for concluído e não tiver bytes ou número de arquivos a serem relatados, será emitida a seguinte mensagem:

ANR0985I Processo *process\_id* para *process\_name* em execução no *process\_state* foi concluído como *completion\_state* às *time*

A lista a seguir define as variáveis a partir desta mensagem:

*process\_id*

Identificador de processo numérico.

*process\_name*

O nome do processo.

*process\_state*

**FOREGROUND** ou **BACKGROUND**. Se o processo estiver em execução no primeiro plano, isto indica que o comando foi emitido com o parâmetro **WAIT=YES**. O processamento em primeiro plano faz a sessão administrativa que emitiu o comando aguardar até a conclusão do processamento. Um processo em execução no segundo plano retorna imediatamente à sessão administrativa que emitiu o comando, indicando que um processo foi iniciado enquanto o processo ainda está em execução. Os processos em execução no segundo plano podem ser monitorados com o comando **QUERY PROCESS**.

*completion\_state*

SUCCESS ou FAILURE.

*time* O horário de início do processo.

## Processo Terminado com Itens e Bytes

Quando um processo for concluído e tiver bytes e itens processados no relatório, será emitida a seguinte mensagem:

ANR0986I 0 processo *process\_id* para *process\_name* em execução no *process\_state* processou *number\_of\_items* itens para um total de *bytes\_processed* bytes com um estado de conclusão *completion\_state* às *time*

A lista a seguir define as variáveis a partir desta mensagem:

*process\_id*

Identificador de processo numérico.

*process\_name*

O nome do processo.

*process\_state*

**FOREGROUND** ou **BACKGROUND**. Se o processo estiver em execução no primeiro plano, isto indica que o comando foi emitido com o parâmetro **WAIT=YES**. O processamento em primeiro plano faz a sessão administrativa que emitiu o comando aguardar até a conclusão do processamento. Um processo em execução no segundo plano retorna imediatamente à sessão administrativa que emitiu o comando, indicando que um processo foi iniciado enquanto o processo ainda está em execução. Os processos em execução no segundo plano podem ser monitorados com o comando **QUERY PROCESS**.

*number\_of\_items*

O número de itens processados.

*bytes\_processed*

O número de bytes processados.

*completion\_state*

SUCCESS ou FAILURE.

*time* O horário de início do processo.

## Processo Terminado com Itens

Quando um processo for concluído e tiver itens processados no relatório, será emitida a seguinte mensagem:

ANR0987I 0 processo *process\_id* para *process\_name* em execução no *process\_state* processou *number\_of\_items* itens com um estado de conclusão *completion\_state* às *time*

A lista a seguir define as variáveis a partir desta mensagem:

*process\_id*

Identificador de processo numérico.

*process\_name*

O nome do processo.

*process\_state*

**FOREGROUND** ou **BACKGROUND**. Se o processo estiver em execução no primeiro plano, isto indica que o comando foi emitido com o parâmetro **WAIT=YES**. O processamento em primeiro plano faz a sessão administrativa que emitiu o comando aguardar até a conclusão do processamento. Um processo em

execução no segundo plano retorna imediatamente à sessão administrativa que emitiu o comando, indicando que um processo foi iniciado enquanto o processo ainda está em execução. Os processos em execução no segundo plano podem ser monitorados com o comando **QUERY PROCESS**.

*completion\_state*

SUCCESS ou FAILURE.

*time* O horário de início do processo.

## Processo Terminado com Bytes

Quando um processo for concluído e tiver bytes processados no relatório, será emitida a seguinte mensagem:

ANR0988I O processo *process\_id* para *process\_name* em execução no *process\_state* processou *bytes\_processed* bytes com um estado de conclusão *completion\_state* às *time*

A lista a seguir define as variáveis a partir desta mensagem:

*process\_id*

Identificador de processo numérico.

*process\_name*

O nome do processo.

*process\_state*

**FOREGROUND** ou **BACKGROUND**. Se o processo estiver em execução no primeiro plano, isto indica que o comando foi emitido com o parâmetro **WAIT=YES**. O processamento em primeiro plano faz a sessão administrativa que emitiu o comando aguardar até a conclusão do processamento. Um processo em execução no segundo plano retorna imediatamente à sessão administrativa que emitiu o comando, indicando que um processo foi iniciado enquanto o processo ainda está em execução. Os processos em execução no segundo plano podem ser monitorados com o comando **QUERY PROCESS**.

*bytes\_processed*

O número de bytes processados.

*completion\_state*

SUCCESS ou FAILURE.

*time* O horário de início do processo.

## Analizando a Mensagem de Erro ANR1221E

Ao receber uma mensagem de erro ANR1221E, geralmente a causa ocorre devido a espaço insuficiente no conjunto de armazenamento da cópia de destino.

### Sobre Esta Tarefa

Execute as seguintes etapas para resolver a mensagem de erro ANR1221E:

### Procedimento

1. Emita o comando **QUERY STGPPOOL** *stgpoolName* **F=D**.
2. Emita a seguinte instrução SQL select a partir de um cliente administrativo para este servidor: "select *stgpool\_name*,*devclass\_name*,*count(\*)* as 'VOLUMES' from volumes group by *stgpool\_name*,*devclass\_name*."
3. Compare o número de volumes relatados pela instrução select com o máximo de volumes utilizáveis permitidos (conforme relatado pelo comando **QUERY STGPPOOL**). Se o número de volumes relatados pelo **select** for igual ou exceder o

“Máximo de Volumes Utilizáveis Permitidos”, atualize o conjunto de armazenamento e permita volumes mais utilizáveis. Se volumes utilizáveis não forem usados no conjunto de armazenamento (utilizável=0), certifique-se de incluir mais volumes privados. Emita o comando `UPDATE STGP00L stgpoolName MAXSCR=nn`, em que *stgpoolName* é o nome do conjunto de armazenamento a ser atualizado e *nn* é o número aumentado de volumes utilizáveis que serão disponibilizados para esse conjunto de armazenamento de cópia.

**Importante:** A biblioteca de fitas deve ter este número adicional de volumes utilizáveis disponíveis ou será necessário incluir volumes utilizáveis na biblioteca antes de emitir este comando e de tentar novamente a operação **BACKUP STGP00L**.

## Analizando a Mensagem de Erro ANR2317W

A mensagem de erro ANR2317W é emitida quando um processo determina que existe um arquivo danificado.

### Sobre Esta Tarefa

A mensagem é mostrada com as seguintes informações:

```
ANR2317W
0 volume de auditoria localizou um arquivo danificado no volume
volumeName: Nó nodeName,
Tipo fileType, Espaço de arquivo fileSpaceName, fsId
fileSpaceID,
0 nome do arquivo fileName é o número version das versões
totalVersions.
```

Execute as seguintes etapas para resolver a mensagem de erro ANR2317W:

### Procedimento

1. Emita o comando **QUERY VOLUME** *volumeName* **F=D**.
2. Emita a seguinte instrução SQL select a partir de um cliente administrativo para este servidor: “select\* from VOLHISTORY where VOLUME\_NAME='volume\_name' AND TYPE='STGNEW.” Os resultados do comando **QUERY VOLUME** indicam quando este volume foi gravado pela última vez. As informações da operação **SELECT** relatam quando este volume foi incluído no conjunto de armazenamentos. Geralmente, **AUDIT VOLUME** pode relatar arquivos como danificados porque no momento que os dados foram gravados, o hardware estava com mau funcionamento e não os gravou corretamente, embora seja relatado ao servidor IBM Spectrum Protect que a operação foi bem-sucedida. Como resultado do mau funcionamento deste dispositivo, muitos arquivos em muitos volumes diferentes podem ser afetados. Execute as seguintes etapas para resolver este problema:
  - a. Avalie os logs de erro de sistema ou outras informações sobre esta unidade para determinar se ainda é relatado um erro. Se ainda forem relatados erros, primeiro eles deverão ser resolvidos. Para resolver um problema de hardware, trabalhe com o fornecedor do hardware para corrigir o problema.
  - b. Se este conjunto de armazenamentos for uma cópia de um volume do conjunto de armazenamentos, apenas exclua este volume usando o comando **DELETE VOLUME** *volumeName* **DISCARDATA=YES**. Na próxima vez em que um backup do conjunto de armazenamentos for executado para o conjunto de armazenamento primário ou conjuntos de armazenamentos nos



quais estes dados danificados residem, será feito um novo backup para este conjunto de armazenamentos de cópia e nenhuma ação adicional será necessária.

- Se este conjunto de armazenamentos for um volume do conjunto de armazenamento primário e se os dados foram gravados diretamente neste volume quando o cliente armazenou os dados, provavelmente não havia cópias não danificadas dos dados no servidor. Se possível, faça backup dos arquivos novamente a partir do cliente.
- Se esse conjunto de armazenamento for um volume do conjunto de armazenamento primário, mas os dados tiverem sido colocados nesse volume pelos comandos **MIGRATION**, **MOVE DATA** ou **MOVE NODEDATA**, poderá haver uma cópia não danificada do arquivo no servidor. Se o conjunto de armazenamento primário que continha esse arquivo tiver backup em um conjunto de armazenamento de cópia anterior aos comandos **MIGRATION**, **MOVE DATA** ou **MOVE NODEDATA**, um arquivo não danificado poderá existir. Se um arquivo não danificado existir, emita o comando **UPDATE VOLUME *volumeName* ACCESS=DESTROYED** e depois emita o comando **RESTORE VOLUME *volumeName*** para recuperar os arquivos danificados desse volume do conjunto de armazenamento de cópia.

## Analizando as Mensagens de Erro ANR1330E e ANR1331E

Você poderá receber a mensagem de erro ANR1330E ou ANR1331E enquanto os dados estão sendo lidos a partir de um volume do conjunto de armazenamentos do IBM Spectrum Protect.

Quando o servidor armazena dados em um volume do conjunto de armazenamentos, informações autoexplicativas são inseridas periodicamente em todos os dados. Essas informações são verificadas quanto à validade enquanto o servidor lê os dados. As mensagens ANR1330E e ANR1331E serão emitidas se a verificação revelar que as informações são inválidas. A mensagem de erro ANR1330E exibe os valores reais que foram lidos, enquanto a mensagem de erro ANR1331E exibe os valores que eram esperados. O servidor emite essas mensagens pelas seguintes razões:

- O hardware (subsistema de disco e unidade de fita) encontrou um problema enquanto os dados eram lidos.
- Ocorreu um erro enquanto os dados estavam sendo gravados e foram danificados.
- Uma operação de restauração de banco de dados foi executada e um volume não foi adequadamente auditorado para que estivesse em sincronização com o horário da restauração point-in-time (PIT).

Primeiro deve-se determinar se os dados estão danificados na mídia ou se ocorreu um erro quando o servidor lia os dados intactos. Emita o seguinte comando para o volume no qual os dados estão armazenados:

```
AUDIT VOLUME FIX=NO
```

Se a auditoria não reportar arquivos danificados, o IBM Spectrum Protect leu com êxito os dados que foram reportados anteriormente como danificados. Nesse caso, o erro foi causado por um mau funcionamento temporário do hardware quando o servidor lia os dados. No entanto, se a auditoria ainda relatar que os dados estão danificados, determine o que causou o dano.

Você pode ignorar o erro, mas apenas se ele ocorrer com pouca frequência. O hardware ocasionalmente encontra um erro ao ler dados. Na maioria dos casos, o

hardware reconhece que ocorreu um erro e efetua a recuperação sem precisar relatá-lo. Mas há vezes em que os dados são lidos em um estado alterado (danificado) por causa de um erro temporário de hardware. A lista a seguir define os resultados de leitura de dados e recebimento de um erro:

#### **Auditoria OK, erro ao ler dados intactos na mídia**

O IBM Spectrum Protect verifica as informações autoexplicativas e reporta os dados como danificados se eles não correspondem ao esperado. Nas mensagens ANR1330E e ANR1331E, os dados são reportados como danificados.

Se após auditar o volume, as mensagens ANR1330E e ANR1331E forem exibidas frequentemente, determine qual dispositivo de hardware está causando a leitura incorreta dos dados. Consulte o log de atividades para descobrir a data e hora em que as mensagens ANR1330E e ANR1331E foram emitidas e forneça as informações à sua equipe de suporte de hardware. Com essas informações, eles poderão examinar os logs de erro de hardware para ver se há operações que possam ter sido concluídas de forma anormal. Além disso, sua equipe de suporte de hardware deve assegurar-se de que a manutenção de drivers de dispositivo e microcódigo para o hardware esteja atualizada.

Um lugar comum para tais erros ocorrerem é em uma área de armazenamento em rede (SAN). Normalmente, esses erros ocorrerão se muitos erros de interrupção de nível de link (LLI) ocorrerem no comutador ou na rede. Erros de LLI indicam que o sistema está sendo executado insatisfatoriamente e sabe-se que fazem com que os dados sejam modificados durante retransmissão. Peça para sua equipe de suporte de hardware examinar os logs de erros da rede para ver se há instâncias de erros de LLI. Procure erros de LLI que foram registrados por volta da hora em que as mensagens ANR1330E e ANR1331E foram emitidas.

#### **Falha de auditoria, dados danificados na mídia**

Se a auditoria reportar os dados como danificados, pode ter ocorrido um erro que fez com que os dados fossem gravados incorretamente na mídia. Além disso, uma operação de restauração de banco de dados pode ter um volume que não foi adequadamente auditorado na sincronização com o horário da restauração PIT. Determine, pelos relatórios de auditoria, quando os dados foram gravados e examine a mensagem ANR1331E para descobrir qual dispositivo de hardware danificou os dados. Consulte o seguinte exemplo de dados:

```
ANR1330E
O servidor detectou possível dano em um objeto sendo restaurado
ou movido. Os valores reais para o quadro incorreto são: magic C6A2D75D
ver hdr 35134 compr. hdr 43170 número de sequência 160421181 compr. dados
7E53DCD8 ID servidor 348145193 ID segmento 327643666840426461 crc 06E04914.
```

```
ANR1331E
Quadro inválido detectado. Esperava-se magic 53454652 número de sequência
00000023 ID do servidor 00000000 ID do segmento 2062.
```

O número do ID do segmento na mensagem ANR1331E neste exemplo é 2062. Para determinar a data em que os dados foram inseridos no servidor, emita o seguinte comando:

```
SHOW INVO 0 2062
```

O exemplo a seguir mostra a saída do comando **SHOW INVO**:

```
OBJECT: 0.2062 (Backup):  
Node: NODE1 Filespace: \\node1\\c$ (Unicode).  
\\5400\\BF\\ BFDEFS.H  
Type: 2 (File) CG: 1 Size: 0.89088 HeaderSize: 364
```

```
BACKUP OBJECTS ENTRY:  
State: 1 Type: 2 MC: 1 CG: 1  
\\node1\\c$ (Unicode) : \\TESTFILES\\ FILE1.TXT (MC: DEFAULT)  
Active, Inserted 11/29/2009 13:28:26  
EXPIRING OBJECTS ENTRY:  
Entrada o objeto expirando não encontrada.
```

Localize o campo Inserted e anote a data e hora. Neste exemplo, o objeto foi inserido no dia 29/11/2009 às 13h28min26s. Forneça à sua equipe de suporte de hardware a data e hora. A equipe de suporte pode examinar os logs de erro de hardware para ver se há operações que foram concluídas de modo anormal. Além disso, solicite que a equipe de suporte assegure que os drivers de dispositivo e a manutenção de microcódigo para o hardware estejam atualizados. Sua equipe de suporte de hardware deve examinar os logs de erros da rede SAN. Procure erros que ocorreram por volta da hora em que os dados foram inseridos no IBM Spectrum Protect.

Se o comando **SHOW INVO** não retornar saída útil, emita o seguinte comando para determinar a data de inserção:

```
SHOW BFO 0 xxx
```

em que xxx é o ID do grupo de segmento. O exemplo mostra a saída do comando **SHOW BFO**:

```
Objeto de Arquivo de Bit: 0.xxx  
**0 super arquivo de bit 0.xxx contém os seguintes arquivos de bit agregados  
(deslocamento/comprimento)  
0.2063 0.75295 0.3071 Ativo  
0.2064 0.78366 0.88780 Ativo  
0.2065 0.167146 0.13831 Ativo  
0.2066 0.180977 0.21254 Ativo  
0.2067 0.202231 0.3808 Ativo  
0.2068 0.206039 0.11261 Ativo
```

```
**Entrada de Arquivo de Bit em Disco  
Tipo de Arquivo de Bit: PRIMARY  
Formato de Armazenamento: 22  
Tamanho Lógico: 0.217364  
Tamanho Físico: 0.221184  
Número de Segmentos: 1,  
Excluído: False  
ID do Conjunto de Armazenamento: 1  
ID do Volume: 2  
Nome do volume: TapeVol1
```

Obtenha um número de arquivo de bit agregado da primeira entrada na lista de arquivos de bit agregados. No exemplo anterior, o primeiro número de arquivo de bit agregado é 2063. Emita o comando **SHOW INVO** usando 2063.

### Nenhum erro de hardware no momento da inserção

Se a equipe de suporte de hardware descobrir que nenhum erro de hardware ocorreu no momento em que os dados eram inseridos no IBM Spectrum Protect, entre em contato com a equipe de suporte IBM. Forneça à equipe o log de atividades no momento em que as mensagens ANR1330E e ANR1331E foram emitidas. Além disso, emita o comando **AUDIT VOLUME FIX=NO** com o seguinte rastreo e forneça o rastreo à equipe de suporte do IBM Spectrum Protect:

```
TRACE ENABLE BF AF DF SS AS DS SSFRAME
TRACE DISABLE BFLOCK AFLOCK SSLOCK
TRACE BEGIN filename
```

### Corrigindo arquivos danificados na mídia

Se você achar que os dados estão danificados em um volume, emita o comando **AUDIT VOLUME FIX=YES** no volume. Se as seguintes condições forem verdadeiras, os dados permanecerão marcados como danificados no volume do conjunto primário:

- O volume é do conjunto primário
- O backup dos dados foi feito em um conjunto de armazenamento de cópia
- Os dados estão danificados

Depois que o comando **AUDIT VOLUME FIX=YES** for emitido, emita o comando **RESTORE VOLUME** para o volume do conjunto primário. Os dados danificados são substituídos por uma nova cópia dos dados. Se o comando **AUDIT VOLUME FIX=YES** ler os dados com êxito, eles não serão mais marcados como danificados no conjunto de armazenamento primário.

Se não houver cópia de backup, o comando **AUDIT VOLUME FIX=YES** excluirá os dados. Se os dados que foram excluídos forem dados de backup, eles serão colocados no servidor na próxima vez que o backup do cliente for executado.

Se os dados que estão sendo excluídos pelo comando **AUDIT VOLUME FIX=YES** estiverem em um volume do conjunto de armazenamento de cópia, eles serão excluídos do volume do conjunto de cópias. Da próxima vez que for feito backup do conjunto de armazenamento primário, uma nova cópia será incluída no conjunto de armazenamento de cópia.

## Os Arquivos Não Expiram após a Redução de Versões

É possível atualizar as políticas do servidor para reduzir o número de versões de um arquivo que você deseja manter; no entanto, às vezes podem ser gerados erros como resultado dessas atualizações.

Emita o comando **QUERY COPYGROUP** *domainName policySetName copyGroupName F=D*. Se os parâmetros **Os Dados de Versões Existem** ou **Dados de Versões Excluídos** foram alterados para um grupo de cópias **TYPE=BACKUP**, isto pode afetar a expiração.

Se os valores **Existem dados de versões** ou **Dados de versões excluídos** para um grupo de cópias **TYPE=BACKUP** forem reduzidos, o processo de expiração do servidor pode não reconhecer imediatamente este fato e o processo pode expirar esses arquivos. O servidor aplica os valores **Existem dados de versões** e **Dados de versões excluídos** aos arquivos somente no momento em que eles receberam backup no servidor. Quando é feito backup de um arquivo, o servidor conta o número de versões desse arquivo, e se for excedido o número de versões que devem ser mantidas, o servidor marcará para expiração as versões mais antigas que excederem este valor.

## Os Sintomas do Processo Indicam Erros de Migração

É possível aparecer sintomas do processo que apontam para a migração como a causa de erros.

### A Migração Não É Executada para o Conjunto de Armazenamentos de Mídia Sequencial

Se a migração não for executada para conjuntos de armazenamentos de mídia sequencial, emita o comando **QUERY STGPPOOL** *stgpoolName* **F=D**.

A migração de conjuntos de armazenamentos de mídia sequencial calcula a “Porcent. Util.” como o número de volumes em uso para o conjunto de armazenamentos, em relação ao número total de volumes que podem ser usados para esse conjunto de armazenamentos. De forma semelhante, ela calcula a “Porcent. Migração” como o número de volumes com dados que podem ser migrados, em uso para o conjunto de armazenamentos, em relação ao número total de volumes que podem ser usados para esse conjunto de armazenamento. Como volumes utilizáveis não utilizados podem estar sendo considerados nesse cálculo, é possível que não apareçam dados suficientes que possam ser migrados no conjunto de armazenamento para o processamento de migração.

### A Migração Usa apenas Um Processo

Emita os comandos **QUERY STGPPOOL** *stgpoolName* **F=D** e **QUERY OCCUPANCY \* \* STGPPOOL=** *stgpoolName*.

A seguir, os motivos pelos quais apenas um processo de migração está executando:

- A configuração de Processos de Migração para o conjunto de armazenamentos está definida como um ou não está definida (em branco). Se verdadeiro, emita o comando **UPDATE STGPPOOL** *stgpoolName* **MIGPROCESS=***n*, em que *n* é o número de processos a serem usados para migração a partir deste conjunto. Observe que este valor deve ser menor ou igual ao número de unidades (limite de montagem) para o PRÓXIMO conjunto de armazenamentos no qual a migração está armazenando dados.
- Se o comando **QUERY OCCUPANCY** relatar apenas um único nó cliente e espaço no arquivo neste conjunto de armazenamentos, a migração poderá executar apenas um único processo, mesmo que a configuração de Processos de Migração para o conjunto de armazenamentos seja maior que um. O processamento de migração está particionando dados, com base no nó cliente e no espaço no arquivo. Para que a migração execute com vários processos, dados para mais de um nó cliente precisam estar disponíveis nesse conjunto de armazenamento.

---

## Resolvendo Problemas do Conjunto de Armazenamentos

Os conjuntos de armazenamentos são essenciais para uma operação do servidor bem-sucedida. O banco de dados do IBM Spectrum Protect contém informações nos conjuntos de armazenamentos sobre nós clientes registrados, políticas, planejamentos e os dados do cliente.

Essas informações devem estar disponíveis e ser válidas para que o IBM Spectrum Protect funcione corretamente. Os erros do conjunto de armazenamentos podem estar relacionados aos seguintes problemas:

- Transações falhas

- Um conjunto de armazenamentos com um alto uso de volume após aumentar o volume MAXSCRATCH
- Um conjunto de armazenamentos tendo “Collocate?=Yes”, mas os volumes ainda contendo dados para muitos nós
- Não é possível armazenar dados em um conjunto de dados ativos usando a função de gravação simultânea ou emitindo o comando **COPY ACTIVATEDATA**

## Recebida a Mensagem “ANR0522W Falha na transação...”

A mensagem ANR0522W é exibida quando o servidor não pode alocar espaço no conjunto de armazenamentos identificado para armazenar dados para o cliente especificado.

### Sobre Esta Tarefa

Existem várias possíveis causas para a falta de espaço em um conjunto de armazenamentos. Execute os seguintes procedimentos para resolver o erro de alocação de espaço:

### Procedimento

1. Emita **QUERY VOLUME volname F=D** para os volumes no conjunto de armazenamentos referido. Para qualquer volume relatado com acesso que não seja de leitura/gravação, verifique esse volume. Um volume pode ser marcado como Somente/Leitura ou Indisponível devido a um erro de dispositivo. Se o erro de dispositivo for resolvido, emita o comando **UPDATE VOLUME volname ACCESS=READWRITE** para permitir que o servidor selecione e tente gravar dados nesse volume.
2. Emita **QUERY VOLUME volname** para os volumes no conjunto de armazenamentos referido. Os volumes que relatam “pendente” para o status do volume são volumes que estão vazios, mas aguardando para serem reutilizados mais uma vez pelo servidor. O tempo de espera é controlado pela configuração de REUSEDELAY para o conjunto de armazenamentos e exibido como “Período de Atraso para Reutilização do Volume” no comando **QUERY STGPPOOL**. Avalie a configuração de REUSEDELAY para este conjunto de armazenamentos e, se apropriado (com base nos critérios de gerenciamento de dados), reduza este valor emitindo o comando **UPDATE STGPPOOL stgpoolname REUSEDELAY=nn**, em que *stgpoolname* é o nome do conjunto de armazenamentos e *nn* é a nova configuração de atraso de reutilização. A chave para fazer a disposição de dados é ter espaço suficiente no conjunto de armazenamento de destino para que o processamento de disposição selecione um volume apropriado. Ter espaço suficiente no conjunto de armazenamento de destino é significativamente influenciado pelo número de volumes utilizáveis em um conjunto de armazenamentos.
3. Emita o comando **QUERY STGPPOOL F=D** para verificar se o ACESSO é leitura/gravação.

## O Conjunto de Armazenamentos Têm Alto Uso de Volume após o Aumento do Valor MAXSCRATCH

Para conjuntos de armazenamento sequenciais, aumentar o valor **MAXSCRATCH** pode fazer o servidor usar mais volumes.

O servidor usa mais volumes do conjunto de armazenamentos neste caso devido ao processamento de disposição. A disposição agrupa dados do usuário para um nó cliente na mesma fita. Durante uma operação de backup ou archive do cliente, se nenhuma fita tiver dados para este nó cliente, o servidor selecionará um volume utilizável para armazenar os dados. Assim, para outros nós clientes que armazenam dados, o servidor novamente seleciona um volume utilizável. A razão pela qual os volumes utilizáveis não são selecionados antes da alteração da configuração de **MAXSCRATCH** é que, se não houver nenhum volume utilizável disponível e nenhum volume preferencial já designado para este nó cliente, o processamento de seleção de volume no servidor ignorará o pedido de disposição e armazenará os dados em um volume disponível.

## O conjunto de armazenamentos está configurado para usar disposição, mas os volumes contêm dados que não estão dispostos

Quando um conjunto de armazenamentos estiver ativado para disposição (o parâmetro **COLLOCATION** está configurado como GROUP, NODE ou FILESPACE), muitos volumes podem conter dados que não estão dispostos.

Existem duas possibilidades para essa situação:

- Os dados foram armazenados em volumes nesse conjunto de armazenamentos antes de ativar o conjunto de armazenamentos para disposição.
- O conjunto de armazenamento foi executado fora das fitas iniciais e armazenou dados no melhor volume possível, embora a solicitação para disposição tenha sido ignorada.

Se dados para múltiplos nós são finalizados no mesmo volume para um conjunto de armazenamentos que estiver ativado para disposição, use uma das seguintes ações:

- Emita o comando **MOVE DATA** para o volume ou volumes afetados. O processo lê os dados a partir do volume especificado e os move para um volume diferente no mesmo conjunto de armazenamentos se:
  - Volumes utilizáveis estão disponíveis ou
  - Volumes com espaço suficiente estão designados para esse nó cliente para dispor seus dados
- Permita a migração para mover todos os dados desse conjunto de armazenamento configurando os limites HIGHMIG e LOWMIG. Permitindo a migração de todos os dados para o conjunto de armazenamentos NEXT, os requisitos de disposição são processados se o seguinte for verdade:
  - O conjunto de armazenamentos NEXT é ativado por disposição
  - O conjunto de armazenamentos NEXT possui volumes utilizáveis suficientes
  - O conjunto de armazenamentos NEXT tem volumes designados para satisfazer os requisitos de disposição
- Emita o comando **MOVE NODEDATA** para os nós clientes cujos dados estão nesse conjunto de armazenamentos. Se volumes utilizáveis estiverem disponíveis ou

volumes com espaço suficiente estiverem designados para esse nó cliente para dispor seus dados, os seguintes eventos acontecerão:

- O processo **MOVE NODEDATA** lê os dados a partir dos volumes nos quais esse nó possui dados
- O processo **MOVE NODEDATA** move os dados para um volume diferente ou para volumes no mesmo conjunto de armazenamentos

A chave para fazer a disposição de dados é ter espaço suficiente no conjunto de armazenamento de destino para que o processamento de disposição selecione um volume apropriado. Deve haver suficientes volumes nulos disponíveis no conjunto de armazenamentos para permitir que a disposição selecione um novo volume. Certifique-se de que suficientes volumes nulos estão disponíveis ao invés de usar um volume que já tenha dados nele a partir de um nó diferente. Volumes nulos podem ser volumes utilizáveis se o conjunto de armazenamentos estiver definido com suficientes volumes utilizáveis ou defina os volumes nulos emitindo o comando **DEFINE VOLUME**.

## Resolvendo Problemas de Armazenamento dos Conjuntos de Dados Ativos

Você pode ter dificuldades ao armazenar dados em um conjunto de dados ativos usando a função de gravação simultânea ou emitindo o comando **COPY ACTIVEDATA**.

Antes do armazenamento dos dados em um conjunto de dados ativos, é necessário estabelecer uma política para permitir os dados no conjunto. O nó que possui os dados deve ser designado a um domínio cujo conjunto de dados ativos está listado no campo **ACTIVEDESTINATION** do domínio. Emita o seguinte comando para determinar se o nó está designado a um domínio que autoriza o armazenamento no conjunto de dados ativos:

```
QUERY NODE node_name F=D
```

O campo Nome de Domínio de Política lista o domínio ao qual o nó está designado. Emita o seguinte comando para determinar se o conjunto de dados ativos está listado no campo **ACTIVEDESTINATION** de domínio:

```
QUERY DOMAIN  
domain_name F=D
```

Se o conjunto de dados ativos não estiver listado, emita o seguinte comando para incluir o conjunto de dados ativos na lista:

```
UPDATE DOMAIN domain_name ACTIVEDESTINATION=active-data_pool_name
```

**Dica:** Depois de emitir o comando **UPDATE DOMAIN *domain\_name* ACTIVEDESTINATION=*active-data\_pool\_name***, todos os nós designados ao domínios serão autorizados a armazenar dados no conjunto de dados ativos. Se autorizar os nós designados ao domínio a armazenar dados não for aceitável, será necessário criar um novo domínio para esses nós, cujos dados você deseja armazenar no conjunto de dados ativos e designar esses nós ao domínio recém-criado.



---

## Resolvendo problemas com conjuntos de armazenamentos de contêiner em nuvem

Com o IBM Spectrum Protect, é possível fazer backup de dados e restaurar dados diretamente de um conjunto de armazenamentos de contêiner em nuvem.

Às vezes, você pode encontrar problemas de desempenho ou limitações com conjuntos de armazenamentos de contêiner em nuvem. Para obter informações adicionais, consulte as FAQs de conjuntos de armazenamentos de contêiner em nuvem no IBM DeveloperWorks.

Use a orientação a seguir para resolver problemas e manipular limitações:

### Problemas com a exclusão de objetos da nuvem

O desempenho de um conjunto de armazenamentos de contêiner em nuvem conta com a conexão de rede entre o servidor e a nuvem. Dependendo do provedor em nuvem, excluir objetos do armazenamento em nuvem pode levar uma quantidade de tempo significativa. Por exemplo, se você estiver usando Swift OpenStack como seu provedor em nuvem, será necessário excluir individualmente objetos de nuvem e a latência de rede impactará cada operação de exclusão. Se você precisar excluir muitos objetos de nuvem em pouco tempo, certifique-se de que IBM Spectrum Protect possa eventualmente excluir todos os objetos salvos na nuvem. Por exemplo, você pode encontrar desempenho insatisfatório se usar um provedor em nuvem fora do local e excluir regularmente espaços no arquivo do IBM Spectrum Protect.

### Removendo dados marcados como danificados ou órfãos durante uma auditoria

Uma extensão de dados danificados é um arquivo que possui referências no banco de dados do servidor, mas possui dados ausentes ou corrompidos na nuvem. Uma extensão de dados órfãos é um objeto armazenado em um provedor de serviços em nuvem que não tem uma referência no banco de dados do servidor. O parâmetro **FORCEORPHANDBDELETE** para o comando **AUDIT CONTAINER** ativa o servidor para forçar a exclusão de extensões órfãs do banco de dados do servidor, mesmo que eles não sejam excluídos do conjunto de armazenamentos de contêiner em nuvem. Este parâmetro é opcional.

### Problemas de desempenho com a restauração de arquivos

Se você encontrar desempenho insatisfatório ao restaurar arquivos, verifique se a operação de restauração está disponível em seu ambiente. Consulte nota técnica 1659833.

### Restrições para conjuntos de armazenamentos de contêiner em nuvem

As seguintes funções não são compatíveis com conjuntos de armazenamentos de contêiner em nuvem:

- Replicação de um conjunto de armazenamentos de contêiner em nuvem com o comando **PROTECT STGPPOOL**
- Migração
- Reclamação
- Agregação
- Disposição
- Operações de gravação simultânea
- Operações de backup do conjunto de armazenamentos
- Uso de volumes virtuais

Além disso, você não pode utilizar o parâmetro **NEXTSTGPOOL** com o comando **DEFINE STGPOOL** em um conjunto de armazenamentos de contêiner em nuvem ou um conjunto de armazenamentos de contêiner de diretório porque o IBM Spectrum Protect não pode determinar quando o provedor de armazenamento em nuvem está cheio. Use o parâmetro **NEXTSTGPOOL** para especificar apenas um conjunto de armazenamentos de acesso aleatório ou sequencial primário. Como resultado, a capacidade de estouro não está disponível para conjuntos de armazenamentos baseados em contêiner.

#### **Nenhum failover para a nuvem após o armazenamento local se torna cheio**

Se você utilizar os diretórios do conjunto de armazenamentos com um conjunto de armazenamentos de contêiner em nuvem, e os diretórios não contiverem mais espaço livre, as operações de backup pararão prematuramente. Para evitar essa situação, aloque mais diretórios do conjunto de armazenamentos para fornecer ao conjunto de armazenamentos mais espaço de armazenamento local para operações de backup. Você também pode aguardar até que os dados sejam automaticamente limpos dos diretórios locais depois que eles forem movidos para a nuvem.

#### **Limitações sobre uso de replicação do nó com um conjunto de armazenamentos de contêiner em nuvem**

É possível usar um conjunto de armazenamentos de contêiner em nuvem como um conjunto de armazenamentos de destino em um servidor de replicação de origem. No entanto, não é possível usar um conjunto de armazenamentos de contêiner em nuvem como um conjunto de armazenamentos de origem em um servidor de replicação de origem. Para fornecer redundância, utilize os recursos de replicação que estão disponíveis a partir do provedor de armazenamento em nuvem.

#### **Os tipos de arquivos para evitar com conjuntos de armazenamentos de contêiner em nuvem**

Para um conjunto de armazenamentos de contêiner em nuvem, evite armazenar tipos de dados do cliente que não sejam otimizados para armazenar dados em conjuntos de armazenamentos de mídias removíveis. Por exemplo, evite armazenar arquivos de controle do Data Protection for VMware e arquivos de metadados do Data Protection for SQL (para backups anteriores de SQL). Para obter mais informações, consulte os seguintes documentos:

- Usando fita, VTL ou conjuntos de armazenamentos de contêiner com o IBM Spectrum Protect for Virtual Environments, nota técnica 1659833
- IT11763: DOCUMENTAÇÃO CONSIDERAÇÕES DE METADADOS ESTÃO AUSENTES NA PROTEÇÃO DE DADOS PARA O SERVIDOR SQL.

---

## Capítulo 4. Resolvendo Problemas do Operations Center

AIX

Linux

Windows

Se ocorrer um problema com o IBM Spectrum Protect Operations Center e você não puder resolvê-lo, poderá consultar as descrições de problemas conhecidos para uma possível solução. Também pode ser necessário revisar os arquivos de log e ativar o rastreo estendido para o Operations Center.

---

### Visão geral de arquivos de log

AIX

Linux

Windows

Se você contatar o suporte de software IBM sobre um problema com o Operations Center, eles poderão solicitar que você envie arquivos de log.

#### Lista de arquivos de log

O Suporte de Software IBM pode solicitar que sejam enviados os seguintes arquivos de log:

- Até oito arquivos de log do Operations Center:

- tsm\_opscntr.log
- tsm\_opscntr1.log
- tsm\_opscntr2.log
- tsm\_opscntr3.log
- tsm\_opscntr4.log
- tsm\_opscntr5.log
- tsm\_opscntr6.log
- tsm\_opscntr7.log

Mais de um arquivo de log do Operations Center pode existir pelas seguintes razões:

- Se o log do Operations Center tiver até 8 MB de tamanho, a versão atual será tsm\_opscntr.log, a versão anterior será tsm\_opscntr1.log, a versão anterior será tsm\_opscntr2.log e assim por diante.
- Se o log do Operations Center for superior a 8 MB de tamanho, o log será difundido por vários arquivos, cada um com um tamanho máximo de 8 MB. Por exemplo, se o log tiver 15 MB de tamanho, ele será difundido para os arquivos tsm\_opscntr.log e tsm\_opscntr1.log.

**Dica:** Se o suporte de software IBM solicitar que você execute um rastreo estendido do Operations Center, poderá identificar quais arquivos de log do Operations Center serão criados durante o rastreo a partir dos horários de modificação dos arquivos.

- Arquivos de log do servidor da web:
  - console.log
  - messages.log
- Arquivos de log de primeira captura de dados com falha (FFDC):
  - exception\_summary\_date\_time.log
  - ffdc\_date\_time.log

## Local de Arquivos de Log

- Os arquivos de log do Operations Center e do servidor da web estarão no seguinte diretório:

**AIX** **Linux** `installation_dir/ui/Liberty/usr/servers/guiServer/logs`

**Windows** `installation_dir\ui\Liberty\usr\servers\guiServer\logs`

em que *installation\_dir* representa o diretório no qual o IBM Spectrum Protect está instalado. Por exemplo:

**AIX** **Linux** `/opt/tivoli/tsm`

**Windows** `c:\Program Files\Tivoli\TSM`

**Dica:** Você também pode visualizar o log do Operations Center de dentro do Operations Center.

- Os arquivos de log FFDC estão no mesmo local, mas no subdiretório `ffdc`.

### Tarefas relacionadas:

“Iniciando um rastreo estendido do Operations Center” na página 119

## Visualizando o log do Operations Center a partir do Operations Center

**AIX** **Linux** **Windows**

O log do Operations Center contém dados de um rastreo de eventos do Operations Center. É possível visualizar o log no Operations Center, ou você pode ir para o diretório que contém o arquivo de log e abrir o arquivo.

### Procedimento

Para visualizar o log do Operations Center enquanto está conectado ao Operations Center, conclua as seguintes etapas:

- Na barra de menus do Operations Center, passe o mouse sobre o ícone de ponto de interrogação e selecione **Sobre o Operations Center**.
- Na janela que é exibida, clique em **Detalhes da instalação**.
- Clique na guia **Visualizar log**.
- Clique em **Exibir log**.

### Tarefas relacionadas:

“Iniciando um rastreo estendido do Operations Center” na página 119

---

## Alertas não São Atualizados Imediatamente

**AIX** **Linux** **Windows**

Na página Alertas do Operations Center, ao tentar designar diversos alertas a um administrador ou fechar diversos alertas, os alertas não são designados ou fechados imediatamente.

## Sintoma

Tabela 8 mostra dados de amostra de um ambiente de teste quando um administrador tiver atualizado vários alertas. Esses resultados podem ser diferentes dos resultados em seu ambiente de armazenamento.

*Tabela 8. Tempos de atraso aproximados quando os alertas foram atualizados em um ambiente controlado*

Número de alertas atualizados	Atraso para alertas do servidor do hub	Atraso para alertas de servidores spoke com o IBM Spectrum Protect Versão 7.1.0	Atraso par alertas a partir dos servidores spoke com a V6.3.4
1	6 segundos	7 segundos	7 segundos
10	6 segundos	7 segundos	9 segundos
100	6 segundos	8 segundos	40 segundos
1.000	10 segundos	20 segundos	5.5 minutos
10.000	45 segundos	1.25 minutos	1 hora

Por exemplo, quando um administrador selecionou 10.000 alertas do servidor do hub e clicou em **Fechar**, levou aproximadamente 45 segundos para que os alertas fossem fechados.

## Solução

Espere até que os alertas sejam atualizados ou atualize menos alertas por vez. Para obter taxas de respostas mais rápidas, faça upgrade dos servidores spoke que estão executando a V6.3.4 para executarem a V7.1 ou posterior.

---

## Tarefas Ativas não São Canceladas Imediatamente

AIX

Linux

Windows

Ao selecionar várias tarefas na página Tarefas ativas do Operations Center e tentar cancelá-las, as tarefas não serão canceladas imediatamente. Há um atraso maior para tarefas do servidor spoke do que para tarefas do servidor do hub.

## Sintoma

Tabela 9 mostra dados de amostra de um ambiente de teste quando um administrador tiver cancelado várias tarefas. Esses resultados podem ser diferentes dos resultados em seu ambiente de armazenamento.

*Tabela 9. Tempos de atraso aproximados quando as tarefas foram canceladas em um ambiente controlado*

Número de tarefas canceladas	Atraso de tarefas do servidor do hub	Atraso para tarefas do servidor spoke
1	5 segundos	5 segundos
10	5 segundos	7 segundos
100	10 segundos	25 segundos
1000	40 segundos	3.5 minutos

Por exemplo, quando um administrador selecionou 1000 tarefas do servidor do hub e clicou em **Cancelar**, levou aproximadamente 40 segundos para que as tarefas fossem canceladas.

## Solução

Espere até que as tarefas sejam canceladas ou cancele menos tarefas por vez.

---

## Problemas Adicionais Conhecidos com o Centro de Operações

AIX

Linux

Windows

Os problemas conhecidos são documentados na forma de notas técnicas na base de conhecimento de Suporte. Conforme os problemas são descobertos e resolvidos, o Suporte de Software IBM atualiza a base de conhecimento. Ao procurar a base de conhecimento, você pode localizar rapidamente as soluções alternativas ou soluções para os problemas.

- Para obter uma lista de problemas conhecidos, consulte a página da web a seguir na Base de conhecimento de suporte: Problemas conhecidos com o IBM Spectrum Protect Operations Center.
- Para obter mais problemas que se tornam conhecidos após a liberação do produto, consulte os resultados da procura a seguir: Resultados da procura para problemas com o IBM Spectrum Protect Operations Center conhecidos.

---

## Capítulo 5. Resolvendo Problemas de Comunicação

A necessidade de conectividade no IBM Spectrum Protect significa que qualquer erro de comunicação pode tornar seu aplicativo inutilizável. Os erros de comunicação podem ser atribuídos à configuração do TCP/IP, a conexões do cliente e do servidor e a outros casos.

---

### Resolvendo Erros Criados ao Conectar-se ao Servidor

Os problemas gerados durante a conexão com o servidor podem estar relacionados às suas opções de comunicação.

Para corrigir o erro, execute qualquer uma ou todas as seguintes opções:

- Revise as mudanças nas opções de comunicação do cliente no arquivo de opções do cliente (se existirem) e tente reverter para os valores anteriores. Tente novamente a conexão.
- Se as configurações de comunicação do servidor foram alteradas, atualize as opções de comunicação do cliente para refletir os valores do servidor alterados ou reverter o servidor para seus valores originais.
- Se algumas configurações de rede foram alteradas, tais como o endereço TCP/IP para o cliente ou servidor (ou um firewall), trabalhe com o administrador de rede para atualizar o cliente, o servidor, ou ambos, para estas mudanças na rede.

---

### Resolvendo Conexões com Falha por Clientes ou Administradores

As duas principais causas para falhas de conexões são falha geral, na qual não é permitida nenhuma conexão, ou uma falha isolada, na qual algumas conexões são permitidas mas outras falham.

Se não for possível nenhuma conexão, poderá ser necessário executar o servidor no primeiro plano para que um console do servidor esteja disponível e as etapas de diagnóstico adicionais possam ser executadas. Verifique as configurações para determinar a configuração apropriada para comunicação com o servidor:

- Certifique-se de que o servidor possa ligar-se a uma porta quando for iniciado. Se não for possível ligar-se a uma porta, provavelmente algum outro aplicativo está usando essa porta. O servidor não poderá ligar-se (usar) a uma determinada porta TCP/IP se outro aplicativo já estiver ligado a essa porta. Se o servidor estiver configurado para comunicações TCP/IP e for ligado com êxito a uma porta na inicialização para sessões do cliente, a seguinte mensagem será emitida:  
ANR8200I Driver TCP/IP pronto para conexão com clientes na porta 1500.

Se um determinado método de comunicação estiver configurado no arquivo de opções do servidor, mas uma mensagem de ligação bem-sucedida não for emitida durante a inicialização do servidor, isto indica que há um problema de inicialização para esse método de comunicação.

- Verifique se a configuração de **TCPPORT** do código no arquivo de opções do servidor está correta. Se a configuração de código tiver sido inadvertidamente alterada, a conexão dos clientes falhará. Isto ocorre porque os clientes estão tentando conectar-se a uma porta TCP/IP diferente da porta na qual o servidor está atendendo.

- Se vários servidores estiverem usando o mesmo endereço TCP/IP, certifique-se de que **TCPPORT** e **TCPADMINPORT** sejam exclusivos para cada servidor. Por exemplo, existem dois servidores no mesmo endereço TCP/IP. O primeiro servidor possui um **TCPPORT** de 1500 e um **TCPADMINPORT** de 1500. O segundo servidor possui um **TCPPORT** de 1501 e um **TCPADMINPORT** de 1500. O primeiro servidor a acessar a porta 1500 bloqueia o outro servidor a partir da porta 1500 e os clientes não podem mais acessar o primeiro servidor. Os clientes administrativos sempre conectam-se ao segundo servidor. Uma melhor opção de portas para cada servidor seria 1500 e 1501 para **TCPPORT**; 1510 e 1511 para **TCPADMINPORT**.
- Verifique se o servidor está ativado para sessões. Emita o comando **QUERY STATUS** e verifique se “Disponibilidade: Ativada” está configurado. Se o resultado indicar “Disponibilidade: Desativada”, emita o comando **ENABLE SESSIONS**.
- Se clientes específicos não puderem conectar-se ao servidor, verifique as configurações de comunicação para esses clientes. Para TCP/IP, verifique as opções **TCPSERVERADDRESS** e **TCPSERVERPORT** no arquivo de opções do cliente.
- Se apenas um nó específico for rejeitado pelo servidor, verifique se o nó não está bloqueado no servidor. Emita o comando **QUERY NODE nodeName**, em que *nodeName* é o nome do nó a ser verificado. Se o resultado indicar “Bloqueado?: Sim”, avalie por que este nó está bloqueado. Os nós podem ser bloqueados apenas usando o comando administrativo **LOCK NODE**. Se for apropriado desbloquear este nó, emita o comando **UNLOCK NODE nodeName**, em que *nodeName* é o nome do nó a ser desbloqueado.
- Se o computador no qual o servidor está executando estiver com problemas de alocação de memória ou recurso, pode não ser possível iniciar novas conexões com o servidor. O problema de alocação de memória ou de recursos pode ser resolvido temporariamente se o servidor for parado e reiniciado ou se o próprio computador for reiniciado. Esta ação é uma solução temporária e o diagnóstico deve continuar para o sistema operacional ou o servidor porque o problema de alocação de memória e recurso pode indicar um erro em ambos.

---

## Resolvendo Erros de Secure Sockets Layer

Os erros de Secure Sockets Layer (SSL) podem ser atribuídos a uma configuração do ambiente incorreta, um certificado do servidor inválido, problemas de conexão, condições fora de sincronização ou outras causas.

Use a orientação a seguir para resolver problemas comuns de cliente para servidor e de servidor para servidor SSL:

### Não conectando ao servidor depois de usar um certificado de autoridade de certificação (CA) adquirido de fornecedor

Se você estiver usando um certificado adquirido de fornecedor e ele não foi incluído no servidor, especifique o certificado raiz como confiável no banco de dados de chaves do servidor. Para incluir o certificado raiz no banco de dados, emita este comando:

```
gsk8capicmd -cert -add -db cert.kdb -pw password
-label name -file .der_file -format ascii
```

### O certificado raiz da CA não foi incluído no cliente

Inclua o certificado raiz como confiável no banco de dados de chaves do cliente:

```
gsk8capicmd -cert -add -db dsmcert.kdb -pw password
-label my CA -file ca.arm -format ascii
```



### Não é possível executar gsk8capicmd.exe (IBM Global Security Kit [GSKit])

Na maioria dos casos, esse erro do Windows é gerado por uma configuração incorreta do ambiente. Configure a variável PATH, conforme instruções, antes de executar o utilitário gsk8capicmd.

### ANS1595E Certificado do servidor inválido

Este erro é relatado quando o certificado do servidor não é conhecido para o cliente ou servidor. O erro “certificado de servidor inválido” pode ocorrer nestas condições:

- O certificado nunca foi importado
- O arquivo de certificado cert256.arm foi corrompido antes da importação do certificado
- O comando para importar o certificado foi inserido incorretamente
- A variável *DSM\_DIR* aponta para o diretório incorreto, que contém um banco de dados de chaves do cliente incorreto (dsmcert.kdb)
- O servidor está configurado para Segurança da Camada de Transporte (TLS) 1.2 mas o cliente não está em um nível suficiente (6.3 é requerido).
- O servidor está configurado para TLS 1.2 mas o cliente importou o arquivo cert.arm em vez do arquivo cert256.arm.
- O servidor está configurado para TLS 1.2 mas o cliente importou o arquivo cert256.arm em vez do arquivo cert.arm.

Repita todas as etapas necessárias para importar o certificado do servidor e verifique a variável *DSM\_DIR*. Para obter informações adicionais sobre a falha, consulte o arquivo dsmerror.log. O log de erros do cliente também poderá conter informações sobre a falha específica do IBM GSKit.

### ANS1592E Falha ao inicializar o protocolo SSL

Este erro ocorre no cliente e indica que a conexão SSL não foi estabelecida. Para obter informações adicionais sobre a falha, consulte o log de erro do cliente. O servidor não aceita sessões SSL na porta na qual o cliente ou o servidor está tentando se conectar. Determine se o cliente ou o servidor aponta para a porta do servidor correta (TCPPort), que pode ser um número de porta diferente do padrão 1500.

### ANR8583E e código de retorno 406 de GSKit

Este erro pode indicar que um cliente que não é ativado por SSL está tentando contatar uma porta SSL. Quando um cliente contata um servidor em uma porta que é definida por SSLTCPPORT ou SSLTCPADMINPORT, o servidor estabelece uma sessão e inicia um “handshake SSL”. Se o cliente não for ativado para SSL, ele não poderá concluir o processo de handshake SSL. A sessão então parece parar, mas atinge o tempo limite por meio da opção IDLEWAIT do servidor ou termina quando o administrador do servidor emite o comando **CANCEL SESSION** para cancelá-la manualmente. O exemplo ilustra uma sessão nesse estado, a partir do servidor:

```
TSM:SERVER1>query session
ANR2017I O administrador SERVER_CONSOLE emitiu o comando: QUERY SESSION
```

Sess Number	Comm. Method	Sess State	Wait Time	Bytes Sent	Bytes Recvd	Sess Type	Platform	Client Name
1	SSL	IdleW	17 S	0	0	Node		

**Importante:** Como o ambiente de computação pode fazer com que o processo de handshake demore, não assuma que o resultado sempre indique um cliente não SSL.

**ANR8583E e o código de retorno 420 de GSKit e ANR8581E com o código de retorno 406 de GSKit ocorrem para a mesma sessão do cliente do IBM Spectrum Protect**

Quando as mensagens do servidor ANR8583E e ANR8581E ocorrem para a mesma sessão do cliente, é provável que o cliente tenha gerado uma mensagem ANS1595E. A mensagem ANS1595E geralmente ocorre enquanto o IBM Spectrum Protect tenta estabelecer uma sessão com o servidor. Se verdadeiro, siga a orientação no manual de mensagens do IBM Spectrum Protect para ANS1595E para eliminar estes erros.

**O TLS ANR3338E está em um nível anterior a 1.2**

Este erro é relatado quando o servidor e o agente de armazenamento tentam se conectar a um protocolo SSL anterior ao TLS 1.2. Para comunicação do servidor e do agente de armazenamento, se a opção SSLDISABLELEGACYTLS for especificada, as sessões de TLS deverão se conectar em um nível mínimo de TLS 1.2 ou a sessão será rejeitada.

**Servidores com definição cruzada sem SSL=YES causa interrupção do servidor**

Se você planeja usar a comunicação SSL, a infraestrutura SSL deverá estar no lugar dos servidores de replicação de origem e destino. Os certificados SSL requeridos devem estar no arquivo de banco de dados de chave que pertence a cada servidor. A função SSL estará ativa se o arquivo de opções do servidor contiver a opção SSLTCPPOUT ou SSLTCPADMINPORT ou se um servidor estiver definido com **SSL=YES** na inicialização.

Uma entrada ocorre quando um certificado adquirido de fornecedor em uso não foi incluído no servidor, ou o certificado CA não foi incluído no cliente. Quando uma sessão SSL é iniciada, a mensagem de inicialização da sessão inclui o número de série do certificado do servidor. Portanto, o certificado que está sendo usado pode ser identificado exclusivamente.

**Referências relacionadas:**

Apêndice C, “Códigos de Retorno do IBM Global Security Kit”, na página 213

## **Recuperando a Senha do Arquivo de Banco de Dados de Chaves**

Se você esqueceu a senha do arquivo de banco de dados de chaves atual, o IBM Spectrum Protect poderá ajudá-lo a recuperá-la.

### **Antes de Iniciar**

Você deve ter privilégios no sistema para administrar a recuperação de senha do arquivo de banco de dados de chaves.

### **Sobre Esta Tarefa**

Conclua as seguintes etapas para recuperar e atualizar a senha do arquivo de banco de dados de chaves:

### **Procedimento**

1. Emita o comando **QUERY SSLKEYRINGPW** para exibir a senha do banco de dados de chaves atual.

2. Emita o seguinte comando para usar o registro do servidor da senha do banco de dados de chaves para atualizar a senha:

```
SET SSLKEYRINGPW password UPDATE=Y
```

em que *password* é a senha recuperada pelo comando **QUERY SSLKEYRINGPW**.

## O que Fazer Depois

**Dica:** Se o arquivo `cert.kdb` não existir, você poderá criar um novo arquivo reiniciando o servidor. O servidor cria um arquivo de banco de dados com a senha antiga e gera um novo certificado autoassinado na inicialização. Se você usar certificados autoassinados, extraia o certificado e instale-o em um sistema do cliente. Se você usar um certificado adquirido de fornecedor, deverá incluí-lo novamente no arquivo de banco de dados de chaves do servidor e reiniciar o servidor.

## Resolução de problemas do banco de dados da chave do certificado

As cópias de backup do arquivo `cert.kdb` asseguram que a Segurança da Camada de Transporte (TLS) é iniciada quando o servidor IBM Spectrum Protect é restaurado. Se você tiver uma cópia de backup, será possível restaurar o arquivo e reiniciar o servidor.

### Procedimento

Para criar uma cópia de backup do banco de dados da chave do certificado, `cert.kdb`, conclua as seguintes etapas:

1. Emita o comando do servidor **DELETE KEYRING** para excluir as informações de senha no banco de dados de chaves do IBM Spectrum Protect.
2. Exclua todos os arquivos `cert.*` restantes.
3. Encerre o servidor.
4. Inicie o servidor. O servidor cria automaticamente um novo arquivo `cert.kdb` e uma entrada correspondente no banco de dados do IBM Spectrum Protect. Se você não emitir o comando **DELETE KEYRING**, na inicialização, o servidor tentará criar o banco de dados de chaves com a senha anterior.
5. Redistribua o novo arquivo `.arm` para todos os clientes de backup-archive que estão usando TLS. Se estiver usando o TLS 1.2, use o arquivo `cert256.arm`. Use o arquivo `cert.arm` se o protocolo TLS usado for anterior a 1.2. Reinstale os certificados de empresa terceirizada no cliente de backup-archive. Se estiver usando um servidor de diretório LDAP para autenticar senhas, inclua o certificado raiz que foi usado para assinar o certificado do servidor LDAP. Se o certificado raiz já é um certificado confiável padrão, não será necessário incluí-lo novamente.

## O que Fazer Depois

Se o arquivo do banco de dados de chave `cert.kdb` não existir, o servidor o criará. Uma ou as duas opções `SSLTCPPORT` e `SSLTCPADMINPORT` devem estar no arquivo de opções do servidor quando o servidor for iniciado. O servidor gera uma senha alterável e também um certificado autoassinado que pode ser extraído para uso de clientes e servidores parceiros de negócios do IBM. Se o arquivo `cert.kdb` existir e o servidor não o criou, uma condição fora de sincronização ocorrerá, impedindo o servidor de configurar a comunicação SSL.



---

## Capítulo 6. Resolvendo Problemas do Agente de Armazenamento

O pode fazer backup e restaurar dados de cliente diretamente para e a partir do armazenamento conectado a SAN usando o agente de armazenamento.

---

### Verificando o Log de Atividades do Servidor para Obter Informações do Agente de Armazenamento

Verifique o arquivo de log de atividades do servidor e consulte os relatórios que aparecem 30 minutos antes e 30 minutos depois do momento do erro.

Os agentes de armazenamento iniciam e gerenciam muitas sessões no servidor. Revise o arquivo do log de atividades do servidor para obter mensagens do agente de armazenamento. Para revisar as mensagens do log de atividades, emita o comando **QUERY ACTLOG**.

Se nenhuma mensagem no arquivo do log de atividades do servidor estiver destinada a esse agente de armazenamento, verifique as configurações de comunicação:

- Emita **QUERY SERVER F=D** no servidor e verifique se o endereço de alto nível (HLA) e o endereço de baixo nível (LLA) configurados para a entrada do servidor que representa este agente de armazenamento estão corretos.
- No arquivo de configuração do dispositivo especificado no arquivo `dsmsta.opt`, verifique se **SERVERNAME**, bem como o HLA e o LLA estão configurados corretamente na linha **DEFINE SERVER**.

Verifique se existem mensagens de erro no servidor para esse agente de armazenamento.

---

### Resolvendo um Erro Causado por Leitura ou Gravação em um Dispositivo

Se o problema for um erro envolvendo a leitura ou gravação de dados de um dispositivo, muitos sistemas e dispositivos gravarão informações em um arquivo de log de erros do sistema.

O arquivo de log de erros de sistema do AIX é `errpt` e, para Windows, é o log de eventos.

Se um dispositivo ou volume usado pelo IBM Spectrum Protect estiver relatando um erro para o arquivo de log de erros do sistema, esse erro provavelmente será um problema de dispositivo. As mensagens de erro gravadas no arquivo de log de erros do sistema podem fornecer informações suficientes para resolver o problema.

Os agentes de armazenamento são vulneráveis, principalmente se as informações de caminho forem alteradas ou não estiverem corretas. Emita o comando **QUERY PATH F=D** no servidor. Para cada um dos caminhos do agente de armazenamento, verifique se as configurações estão corretas. Em específico, verifique se o dispositivo listado corresponde ao nome do dispositivo do sistema. Se as informações de caminho não estiverem corretas, atualize-as emitindo o comando

---

## Resolvendo Problemas Causados pela Mudança de Opções do Agente de Armazenamento

As mudanças em opções no arquivo de opções do agente de armazenamento podem causar falha nas operações, mesmo que tenham sido bem-sucedidas anteriormente.

Revise as mudanças no arquivo de opções do agente de armazenamento. Tente reverter as configurações para seus valores originais e tente novamente a operação. Se o agente de armazenamento agora funciona corretamente, tente reintroduzir mudanças no arquivo de opções do agente de armazenamento, uma por vez e tente novamente as operações do agente de armazenamento até que a mudança no arquivo de opções que causou a falha seja identificada.

---

## Resolvendo Problemas Causados pela Mudança de Opções ou Configurações do Servidor

As mudanças nas opções no arquivo de opções do servidor ou mudanças nas configurações do servidor usando os comandos **SET** podem afetar o agente de armazenamento.

Revise as mudanças nas configurações da opção do servidor. Tente reverter as configurações para seus valores originais e tente novamente a operação. Se o agente de armazenamento agora funciona corretamente, tente reintroduzir mudanças no arquivo de opções do agente de armazenamento, uma por vez e tente novamente as operações do agente de armazenamento até que a mudança no arquivo de opções que causou a falha seja identificada.

Revise as configurações do servidor emitindo o comando **QUERY STATUS**. Se as configurações relatadas por esta consulta foram alteradas, revise a razão da mudança e, se possível, reverta-a para o valor original e tente novamente a operação do agente de armazenamento.

---

## Configuração sem a LAN do Agente de Armazenamento

A movimentação de dados sem LAN é a movimentação direta de dados do cliente entre um computador do cliente e um dispositivo de armazenamento em uma SAN, em vez de em uma LAN. É possível ocorrerem problemas com o agente de armazenamento que estejam relacionados à configuração sem a LAN.

### Resolvendo o Problema de Envio de Dados Diretamente para o Servidor

As estatísticas de resumo do cliente não relatam nenhum byte transferido sem a LAN.

#### Antes de Iniciar

O cliente relata os bytes enviados sem a LAN emitindo o comando **"ANE49711 Bytes de Dados sem a LAN: xx KB"**. De forma semelhante, o servidor não relata nenhuma instância de **"ANR0415I Sessão SESS\_NUM com proxy por STORAGE\_AGENT iniciada para o nó NODE\_NAME"** para este nó e agente de armazenamento, indicando que a operação de proxy sem a LAN foi executada para este nó cliente.

O cliente só tentará enviar dados sem LAN com o agente de armazenamento se o destino do conjunto de armazenamentos primários na hierarquia do armazenamento do servidor for sem a LAN. Um conjunto de armazenamento do servidor é ativado para sem LAN em um determinado agente de armazenamento quando um ou mais caminhos são definidos a partir desse agente de armazenamento para um dispositivo SAN.

## Sobre Esta Tarefa

Para determinar se o destino do conjunto de armazenamentos está configurado corretamente, execute os seguintes procedimentos:

### Procedimento

1. Emita o comando **QUERY NODE** *nodeName* para relatar o domínio de política ao qual este nó designado.
2. Emita o comando **QUERY COPYGROUP** *domainName policySetName mgmtclassName F=D* para as classes de gerenciamento que este nó usaria a partir de seu domínio de política designado. Observe que este comando relata informações para arquivos de backup. Para consultar informações do grupo de cópia para arquivos archives, emita o comando **QUERY COPYGROUP** *domainName policySetName mgmtclassName TYPE=ARCHIVE F=D*.
3. Emita o comando **QUERY STGPPOOL** *stgpoolName*, em que *stgpoolName* é o destino relatado das consultas **QUERY COPYGROUP** anteriores.
4. Emita o comando **QUERY DEVCLASS** *deviceClassName* para a classe de dispositivo usada pelo conjunto de armazenamentos de destino.
5. Emita o comando **QUERY LIBRARY** *libraryName* para a biblioteca relatada para a classe de dispositivo usada pelo conjunto de armazenamentos de destino.
6. Emita o comando **QUERY DRIVE** *libraryName F=D* para a biblioteca especificada para a classe de dispositivo usada pelo conjunto de armazenamentos de destino. Se nenhuma unidade estiver definida para esta biblioteca, revise a configuração da biblioteca e da unidade desse servidor e emita o comando **DEFINE DRIVE** para definir as unidades necessárias. Se uma ou mais unidades relatarem "ONLINE=No", avalie porque a unidade está offline e, se possível, atualize-a para online emitindo o comando **UPDATE DRIVE** *libraryName driveName ONLINE=YES*.
7. Emita o comando **QUERY SERVER** para determinar o nome do agente de armazenamento conforme definido para este servidor.
8. Emita o comando **QUERY PATH** *stgAgentName*, em que *stgAgentName* é o nome do agente de armazenamento definido para este servidor e relatado no comando **QUERY SERVER**. Revise esta saída e verifique se um ou mais caminhos estão definidos para unidades definidas para a classe de dispositivo usada pelo conjunto de armazenamentos de destino. Se nenhum caminho estiver definido para este conjunto de armazenamento, emita o comando **DEFINE PATH** para definir os caminhos necessários. Revise também esta saída e verifique se o caminho está on-line. Se os caminhos estiverem definidos, mas nenhum caminho estiver on-line, atualize o caminho para on-line emitindo o comando **UPDATE PATH** *srcName destName SRCTYPE=SERVER DESTTYPE=DRIVE ONLINE=YES*.

## Resolvendo um Conjunto de Armazenamento Ativado Sem a LAN Desqualificado

O servidor desqualifica um conjunto de armazenamento de ser um conjunto de armazenamento sem LAN se ele tiver sido configurado para operações de gravação simultâneas.

Nesse caso, os dados do cliente são enviados diretamente para um servidor que não estará usando um conjunto de armazenamento sem LAN.

Emita o comando **QUERY STGPPOOL** *stgpoolName* **F=D** para o conjunto de armazenamentos de destino para este cliente. Se o conjunto de armazenamento estiver configurado para operações de gravação simultânea, o valor “Conjunto(s) de Armazenamento de Cópia:” fará referência a um ou mais dos outros nomes de conjunto de armazenamento e o IBM Spectrum Protect interpretará a operação de gravação simultânea como tendo uma prioridade mais alta do que a transferência de dados sem a LAN. Como as operações de gravação simultâneas são consideradas de mais alta prioridade, esse conjunto de armazenamento não será relatado como ativado para sem LAN e, portanto, o cliente enviará os dados diretamente para o servidor. O agente de armazenamento não suporta operações de gravação simultânea.

## Assegurando que os Dados Sejam Transferidos Usando um Ambiente sem a LAN

O agente de armazenamento e o cliente podem gerenciar o failover diretamente no servidor, dependendo da configuração sem LAN e do tipo de erro encontrado.

Devido a este recurso de failover, pode não ficar aparente que os dados estão sendo transferidos através da LAN quando era para serem transferidos sem a LAN. É possível configurar o ambiente sem a LAN para limitar a transferência de dados para apenas sem a LAN.

Para testar uma configuração sem LAN, emita o comando **UPDATE NODE** *nodeName* **DATAWRITEPATH=LAN-FREE** para o nó cliente cuja configuração sem LAN você deseja testar. Em seguida, tente uma operação de armazenamento de dados como backup ou restauração. Se o cliente e o agente de armazenamento tentarem enviar os dados diretamente para o servidor usando a LAN, a seguinte mensagem de erro será recebida:

ANR0416W Sessão *sessionNumber* para o nó *nodeName* não permitida para *operation* usando *path* o caminho de transferência de dados

A *operation* relatada indica READ ou WRITE, dependendo da operação tentada. O caminho é relatado como sem a LAN.

Se esta mensagem for recebida quando você estiver tentando um operação sem a LAN, avalie e verifique as configurações sem a LAN. Geralmente, se os dados não forem enviados sem a LAN quando o cliente estiver configurado para usar o recurso sem a LAN, o destino do conjunto de armazenamentos para a política designada a este nó não será um conjunto de armazenamentos ativado sem a LAN, ou os caminhos não serão definidos corretamente.



---

## Capítulo 7. Usando o Rastreo para Resolver Problemas

Às vezes, o IBM Spectrum Protect pode ter problemas que você pode resolver através de rastreo.

---

### Iniciando um rastreo estendido do Operations Center

AIX

Linux

Windows

Por padrão, o log do Operations Center contém dados de um rastreo básico de eventos do Operations Center. O Suporte de Software IBM pode solicitar que você inicie um rastreo estendido.

#### Sobre Esta Tarefa

Para iniciar um rastreo estendido do Operations Center, conclua os seguintes procedimentos:

##### Conceitos relacionados:

“Visão geral de arquivos de log” na página 105

##### Tarefas relacionadas:

“Visualizando o log do Operations Center a partir do Operations Center” na página 106

### Rastreando o Operations Center ativando funções de criação de log a partir do Operations Center

AIX

Linux

Windows

A partir do Operations Center, é possível ativar funções de criação de log e iniciar um rastreo estendido que inclui dados de resolução de problemas no log do Operations Center.

#### Sobre Esta Tarefa

No procedimento a seguir, você ativa grupos de funções de criação de log e inicia um rastreo estendido.

**Atenção:** Certifique-se de desativar os grupos após o rastreo. Caso contrário, o desempenho do Operations Center poderá ser afetado.

#### Procedimento

Para rastrear o Operations Center, conclua as seguintes etapas:

1. Na barra de menus do Operations Center, passe o mouse sobre o ícone de ponto de interrogação e selecione **Sobre o Operations Center**.
2. Clique em **Detalhes da instalação**.
3. Clique na guia **Criação de log**.
4. Na lista de grupos de criação de log, selecione somente as linhas que o Suporte de Software IBM solicita que sejam selecionadas e clique em **Ativar**.
5. Confirme se deseja ativar os grupos de criação de log e clique em **Fechar**.

6. Recrie o problema que está sendo resolvido. O Operations Center é rastreado automaticamente, e uma nova versão do log do Operations Center é criada.
7. Retorna à lista de grupos de criação de log, repetindo a etapa 1 na página 119 - etapa 3 na página 119.
8. Selecione todas as linhas que estão ativadas e clique em **Desativar**.
9. Confirme se deseja desativar os grupos de criação de log e clique em **Fechar**.

## O que Fazer Depois

Para o local e os nomes dos arquivos de log do Operations Center, consulte “Visão geral de arquivos de log” na página 105.

### Tarefas relacionadas:

“Visualizando o log do Operations Center a partir do Operations Center” na página 106

“Rastreando o Operations Center ativando funções no arquivo de configuração de criação de log”

## Rastreando o Operations Center ativando funções no arquivo de configuração de criação de log

AIX

Linux

Windows

Se o problema que está sendo resolvido impedi-lo de abrir o Operations Center, será possível abrir e modificar o arquivo de configuração de criação de log e iniciar o rastreo estendido que inclui dados no log do Operations Center.

### Sobre Esta Tarefa

No procedimento a seguir, você ativa grupos de funções de criação de log e inicia um rastreo estendido.

**Atenção:** Certifique-se de desativar os grupos após o rastreo. Caso contrário, o desempenho do Operations Center poderá ser afetado.

### Procedimento

Para rastrear o Operations Center, conclua as seguintes etapas:

1. Pare o servidor da web do Operations Center.
2. Acesse o seguinte diretório:

AIX

Linux

`installation_dir/ui/Liberty/usr/servers/guiServer`

Windows

`installation_dir\ui\Liberty\usr\servers\guiServer`

em que *installation\_dir* representa o diretório no qual o IBM Spectrum Protect está instalado.

3. Salve uma cópia do arquivo de configuração de criação de log, `OpsCntrLog.config`, em outro local para uso posterior.
4. Abra o arquivo `OpsCntrLog.config` original em um editor de texto.
5. No editor de texto, ative somente os grupos de criação de log que o Suporte de Software IBM solicita que sejam ativados, substituindo a palavra OFF pela palavra ON para cada grupo relevante.
6. Salve e feche o arquivo.
7. Inicie o servidor da web do Operations Center.

8. Recrie o problema que está sendo resolvido. O Operations Center é rastreado automaticamente, e uma nova versão do log do Operations Center é criada.
9. Pare o servidor da web do Operations Center.
10. Retorne ao diretório guiServer.
11. Desative os grupos de criação de log substituindo o arquivo OpsCntrLog.config editado pela cópia salva anteriormente.
12. Inicie o servidor da web do Operations Center.

## O que Fazer Depois

Para obter o local e nomes de arquivos de log do Operations Center, consulte “Visão geral de arquivos de log” na página 105.

### Tarefas relacionadas:

“Rastreamento do Operations Center ativando funções de criação de log a partir do Operations Center” na página 119

---

## Ativando um Rastreamento para o Servidor ou Agente de Armazenamento

É possível emitir comandos de rastreamento dos seguintes locais: console do servidor, console do agente de armazenamento, cliente administrativo conectado ao servidor ou agente de armazenamento, arquivo de opções do servidor (dsmserv.opt) ou arquivo de opções do agente de armazenamento (dsmsta.opt).

### Antes de Iniciar

Os comandos de rastreamento se aplicam ao servidor ou ao agente de armazenamento para o qual o comando foi submetido. Os comandos de rastreamento nos arquivos de opções são usados para rastrear os aplicativos durante a inicialização ou para fornecer um conjunto padrão de classes de rastreamento. Existe uma classe de rastreamento (**ADDMSG**) que sempre é ativada por padrão, se ela aparecer ou não no arquivo de opções. É melhor rastrear para um arquivo. Geralmente, o rastreamento para o servidor ou agente de armazenamento gerará uma grande quantidade de saída.

### Sobre Esta Tarefa

Execute as seguintes etapas para ativar classes de rastreamento para o servidor ou agente de armazenamento.

### Procedimento

1. Determine as classes de rastreamento a serem ativadas. Para que as mensagens de rastreamento sejam emitidas para uma determinada classe de rastreamento, essa classe de rastreamento precisa ser ativada antes do início do rastreamento ou após o início do rastreamento.
2. Emita o comando **TRACE ENABLE** *traceClassName* para ativar uma ou mais classes de rastreamento. Observe que *traceClassName* pode ser uma lista de classes de rastreamento delimitada por vírgulas. Por exemplo, este comando pode ser inserido como **TRACE ENABLE TM SESSION**. O comando **TRACE ENABLE** é acumulativo, de forma que as classes de rastreamento extras podem ser ativadas emitindo o comando **TRACE ENABLE** várias vezes. Por exemplo, se você quiser incluir a classe de rastreamento PVR além daquela que já está ativada, emita: **TRACE ENABLE PVR**. Para parar a emissão de mensagens de rastreamento de uma determinada classe de rastreamento, essa classe de rastreamento precisa ser desativada antes do início do rastreamento ou depois que ele começar.

3. Emita o comando **TRACE DISABLE**<*traceClassName*> para desativar uma ou mais classes de rastreo. Observe que *nome da classe de rastreo* pode ser uma lista de classes de rastreo delimitada por espaço. Por exemplo, este comando pode ser inserido como **TRACE DISABLE TM SESSION**. Classes de rastreo adicionais também podem ser desativadas emitindo **TRACE DISABLE**. Por exemplo, se você desejar remover a classe de rastreo PVR além das que já estavam desativadas, emita: **TRACE DISABLE PVR**. Emitindo **TRACE DISABLE** sem especificar nenhuma classe de rastreo, todas as classes de rastreo atualmente ativadas serão desativadas.
  4. O rastreo pode ocorrer no console ou em um arquivo. Execute as seguintes tarefas para iniciar o rastreo:
    - Para rastreo no console, emita: **TRACE BEGIN**
    - Para rastreo em um arquivo sem limitação de tamanho, emita: **TRACE BEGIN**  
*fileName*
    - Para rastreo em um arquivo com limitação de tamanho, emita: **TRACE BEGIN**  
*fileName* **MAXSIZE=** *tamanho máximo em megabytes*
- Nota:** O *fileName* pode ser um caminho completo, por exemplo, /opt/tmp ou c:\temp. Se um caminho completo não for especificado, o arquivo de rastreo será localizado no mesmo diretório que o arquivo executável em execução.
5. Execute a operação que está causando o problema.
  6. Emita o comando **TRACE END** para parar a emissão de mensagens de rastreo. Se o rastreo estiver sendo feito em um arquivo, finalizá-lo gravará todas as mensagens de rastreo restantes no arquivo e fechará o arquivo.

## O que Fazer Depois

É possível ativar o rastreo e iniciá-lo usando o arquivo de opções do servidor ou do agente de armazenamento. Os comandos e sintaxe discutidos são exatamente os mesmos para o arquivo de opções do servidor ou do agente de armazenamento e, geralmente, eles são usados para rastrear a inicialização do servidor. Por exemplo, se as seguintes linhas foram incluídas no arquivo de opções do servidor, o rastreo será iniciado para as classes de rastreo DB, TM e LOG e as mensagens de rastreo gravadas no arquivo MYTRACE.OUT.

```
TRACE ENABLE DB TM LOG
TRACE BEGIN MYTRACE.OUT BUFSIZE=4096
```

**Lembre-se:** Se você estiver conduzindo um rastreo devido a uma paralisação do servidor, não configure o parâmetro **BUFSIZE**.

### Referências relacionadas:

“Classes de Rastreo para um Servidor ou Agente de Armazenamento” na página 124

## Ativando um Rastreio de Pilha para Mensagens para o Servidor ou Agente de Armazenamento

Um rastreio de pilha revela informações sobre um aplicativo que o Suporte de Software IBM pode usar para ajudar a diagnosticar seus problemas mais rapidamente.

**Nota:** Dependendo da frequência da falha, o rastreio de pilha pode saturar o arquivo de log de atividade, o que pode causar problemas quando você tentar visualizar o arquivo de log de atividade. Talvez você queira desativar o rastreio de pilha após sua conclusão.

O Suporte de Software IBM pode achar útil ativar o rastreio de pilha em mensagens específicas que são emitidas pelo servidor ou agente de armazenamento. Os tipos de mensagens nos quais um rastreio de pilha pode ser ativado são console do servidor, console do agente de armazenamento e o cliente administrativo que está conectado ao servidor ou agente de armazenamento.

Para obter um rastreio de pilha quando uma mensagem específica for emitida pelo servidor ou agente de armazenamento, ative a mensagem para rastreio de pilha. Emita o comando **MSGSTACKTRACE ENABLE** *<messageNumber>* para ativar uma ou mais mensagens para o rastreio de pilha.

**Lembre-se:** *<messageNumber>* pode ser uma lista de números de mensagens delimitada por espaço.

Este comando pode ser inserido como **MS ENABLE 2017**. O comando **MSGSTACKTRACE ENABLE** é acumulativo, de forma que as mensagens extras são ativadas emitindo o comando **MSGSTACKTRACE ENABLE** mais vezes. Se desejar incluir a mensagem 985, além das mensagens que já estão ativadas, emita **MS ENABLE 985**. Observe que apenas a parte do número da mensagem é permitida no comando **MSGSTACKTRACE**. Para parar de obter rastreio de pilha para mensagens que são emitidas pelo servidor ou agente de armazenamento, o rastreio de pilha para essas mensagens deve ser desativado. Emita o comando **MSGSTACKTRACE DISABLE** *<messageNumber>* para desativar uma ou mais mensagens.

O *<messageNumber>* pode ser uma lista delimitada por espaço de números de mensagens. Por exemplo, este comando pode ser inserido como **MSGSTACKTRACE DISABLE 2017 985**. As mensagens extras também podem ser desativadas emitindo **MS DISABLE**. Por exemplo, se desejar remover o número da mensagem 7837, além das mensagens que já estão desativadas, emita o comando **MSGSTACKTRACE DISABLE 7837**.

Por padrão, as seguintes mensagens são ativadas para o rastreio de pilha.

435 437 486 661 685 727 728 780 781 782  
784 785 786 790 793 794 860 881 882 883  
884 1032 1078 1092 1117 1156 1227 5010 5015 5019  
5021 5093 5099 5100 5267 6753 7823 7837 9600 9601  
9602 9604 9605 9606 9607 9608 9999

## Classes de Rastreio para um Servidor ou Agente de Armazenamento

O servidor e o agente de armazenamento fornecem classes de rastreio agregadas. Essas classes de rastreio são um atalho para usar muitas classes de rastreio relacionadas especificando o nome da classe de rastreio agregada para o comando **TRACE ENABLE**.

As classes de rastreio que estão listadas na Tabela 10 são as classes de rastreio que geralmente são mais solicitadas ou usadas para diagnosticar problemas. Esta tabela não inclui todas as classes de rastreio possíveis que estão disponíveis. O nome da classe de rastreio é usado com os comandos **TRACE ENABLE** e **TRACE DISABLE**.

*Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento*

Classes de Rastreio	descrição	Uso
ADDMSG	Emite mensagens do console, como mensagens ANR e ANE para o arquivo de rastreio.	Esta classe de rastreio é importante para correlacionar mensagens do servidor com mensagens de rastreio e para preservar a sincronização de quando cada uma foi emitida.
ADMCMD	Rastreios relacionados ao processamento de comando.	Use esta classe de rastreio para depurar o interpretador de comandos, incluindo a manipulação dos comandos <b>PARALLEL</b> e <b>SERIAL</b> .
AF	Esta classe de rastreio exibe informações sobre dados do usuário que são armazenados em dispositivos de mídia sequencial. AF é uma classe de rastreio agregada que usa AFCREATE, AFMOVE, AFLOCK, AFTXN e AFCOPY. Emita <b>TRACE DISABLE AFLOCK</b> , a menos que as informações de bloqueio sejam explicitamente solicitadas ou necessárias.	Use esta classe de rastreio para diagnosticar problemas de leitura ou gravação de arquivos do usuário em volumes de mídia sequencial.
AFCREATE	Esta classe de rastreio exibe informações sobre como armazenar dados do usuário em volumes de mídias sequenciais.	Use esta classe de rastreio para diagnosticar problemas ao gravar dados do usuário em volumes de mídias sequenciais.
AFMOVE	Esta classe de rastreio exibe operações que movem dados do usuário com volumes de mídias sequenciais. As operações de movimentação são concluídas pelos processos do servidor MIGRATION, RECLAMATION, MOVE DATA e MOVE NODEDATA.	Use esta classe de rastreio para diagnosticar problemas com os processos do servidor de movimentação de dados.

Tabela 10. Classes de Rastreo do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreo	descrição	Uso
AS	Esta classe de rastreo exhibe informações sobre a seleção e designação de volume, coordenação de unidades (pontos de montagem) e gerenciamento de posicionamento de dados em volumes. Essa classe de rastreo agregada usa ASALLOC, ASRTRV, ASDEALLOC, ASMOUNT, ASVOL, ASTXN e ASSD. O método típico é emitir TRACE DISABLE ASTXN, a menos que as informações de bloqueio sejam explicitamente solicitadas ou necessárias.	Use esta classe de rastreo para diagnosticar muitos problemas diferentes sobre volumes, pontos de montagem ou operações de leitura e gravação de dados.
ASALLOC	Esta classe de rastreo exhibe informações sobre como reservar e alocar espaço em volumes de mídias sequenciais para armazenar dados. Este espaço é para o armazenamento de dados em nome de uma sessão do cliente ou para operações de movimentação de dados do servidor, como MIGRATION, RECLAMATION, MOVE DATA ou MOVE NODEDATA.	Diagnostique problemas nos quais o servidor ou o agente de armazenamento relata que não há espaço disponível, mas que o espaço deve estar disponível na hierarquia de armazenamento.
ASDEALLOC	Esta classe de rastreo exhibe informações sobre como liberar e desalocar espaço em volumes de mídias sequenciais para armazenar dados. Geralmente, as operações de desalocação no servidor são <b>EXPIRATION, MIGRATION, RECLAMATION, MOVE DATA, MOVE NODEDATA, AUDIT VOLUME, DELETE VOLUME e DELETE FILESPACE.</b>	Use esta classe de rastreo para diagnosticar problemas durante a exclusão de dados.
ASMOUNT	Esta classe de rastreo exhibe informações sobre a seleção e designação de unidade (ponto de montagem) para dispositivos de mídias sequenciais.	Diagnostique situações nas quais sessões ou processos aguardam por pontos de montagens ou casos nos quais uma operação falha porque nenhum ponto de montagem está disponível. Também é útil nos casos nos quais um ponto de montagem é influenciado.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
ASRTRV	Esta classe de rastreio exibe informações sobre como ler dados de volumes de mídias sequenciais.	Use esta classe de rastreio para diagnosticar problemas sobre dados, como <b>RESTORE</b> ou <b>RETRIEVE</b> client pelo cliente ou <b>MIGRATION</b> , <b>RECLAMATION</b> , <b>STORAGE POOL BACKUP</b> , <b>AUDIT VOLUME</b> , <b>GENERATE BACKUPSET</b> , <b>EXPORT</b> , <b>MOVE DATA</b> ou <b>MOVE NODEDATA</b> pelo servidor.
ASTXN	Esta classe de rastreio exibe informações sobre transações que são usadas para fazer atualizações de banco de dados em informações para volumes de mídia sequencial, conjuntos de armazenamentos, classes de dispositivo e outros atributos.	Use esta classe de rastreio para diagnosticar interrupções, operações do banco de dados, falhas relatadas para operações de mídias sequenciais ou problemas gerais de armazenamento de dados.
ASVOL	Esta classe de rastreio exibe informações sobre a seleção e designação de volume para volumes de mídias sequenciais.	Use esta classe de rastreio para diagnosticar situações nas quais sessões ou processos estão aguardando volumes ou casos em que uma operação falha porque nenhum volume está disponível. Também é útil nos casos nos quais o acesso ao volume é influenciado.
ASSD	Esta classe de rastreio exibe informações sobre operações de dados em fluxo sequencial. Essas operações usam classes de dispositivo de mídia sequencial, volumes ou pontos de montagem, mas não armazenam dados na hierarquia de armazenamento. Os processos do servidor que concluem operações de dados de fluxo sequencial são <b>BACKUP DB</b> , <b>EXPORT/IMPORT</b> e <b>GENERATE BACKUPSET</b> .	Use esta classe de rastreio para diagnosticar processos do servidor que concluem operações de dados de fluxo sequencial.
BF	Informações sobre dados do usuário (arquivos) armazenados na hierarquia de armazenamento. Esta classe de rastreio agregada usa <b>BFCREATE</b> , <b>BFRTV</b> , <b>BFSALVAGE</b> , <b>BFLOCK</b> , <b>BFAGGR</b> , <b>BFREMOTE</b> , <b>BFSAGGR</b> e <b>BFTRG</b> .	Use esta classe de rastreio para diagnosticar problemas de leitura ou gravação de dados gerais para operações do cliente e processos do servidor.



*Tabela 10. Classes de Rastreo do Servidor ou do Agente de Armazenamento (continuação)*

Classes de Rastreo	descrição	Uso
BFAGGR	Esta classe de rastreo exibe informações sobre a agregação do servidor de dados do usuário. O servidor agrega muitos arquivos menores do usuário em um arquivo maior na hierarquia de armazenamento para otimizar o desempenho das operações de movimentação de dados, como <b>MIGRATION</b> , <b>MOVE DATA</b> e <b>MOVE NODEDATA</b> .	Use esta classe de rastreo para diagnosticar problemas de leitura ou gravação de dados gerais para operações do cliente e processos do servidor, ou ambos.
BFCREATE	Esta classe de rastreo exibe informações sobre operações do cliente que armazenam dados na hierarquia de armazenamento. Geralmente, essas operações do cliente são as operações <b>BACKUP</b> , <b>ARCHIVE</b> , ou <b>SPACE MANAGE</b> pelo cliente.	Use esta classe de rastreo para diagnosticar falhas ou outros problemas enquanto o cliente está armazenando dados.
BFREMOTE	Rastreia o primeiro estágio dos processos de backup e restauração de NDMP (Protocolo de Gerenciamento de Dados de Rede).	Esta classe de rastreo é usada para identificar operações de backup ou restauração relacionadas ao NDMP. Estas classes de rastreo são específicas das funções que implementam o protocolo NDMP. A classe de rastreo SPID fornece rastreo mais detalhado, incluindo o rastreo de todos os registros de histórico do arquivo NDMP que são enviados pelo servidor de arquivos NDMP.
BFRTV	Esta classe de rastreo exibe informações sobre operações de cliente que lêem dados da hierarquia de armazenamento.	Use esta classe de rastreo para diagnosticar falhas ou outros problemas enquanto o cliente está lendo dados.
BFSAGGR	Esta classe de rastreo exibe informações sobre o armazenamento, recuperação e movimentação de superagregados. Um objeto maior que 10 GB é armazenado como um a superagregado.	Use esta classe de rastreo para diagnosticar problemas que estão relacionados ao armazenamento ou recuperação de objetos maiores que 10 GB.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
BITVECTOR	Diagnostica problemas em que o servidor relata problemas com conjuntos de armazenamento em disco.	Use esta classe de rastreio para exibir informações sobre como reservar e alocar espaço em volumes em conjuntos de armazenamento em disco.
BKSET/OBJSET	Classe de rastreio para funções do conjunto de backup. As classes de rastreio BKSET e OBJSET são sinônimas.	Use esta classe de rastreio para depurar problemas no comando GENERATE BACKUPSET ou durante uma operação de restauração do cliente de um conjunto de backup.
BLKDISK	Classe de rastreio para visualizar a atividade de E/S do disco no conjunto de armazenamentos, banco de dados e volumes de log.	Use esta classe de rastreio para visualizar a atividade de E/S no disco para diagnosticar erros de desempenho e de E/S do disco.
BRNODE	Classe de rastreio para os comandos <b>BACKUP</b> e <b>RESTORE NODE</b> , que são usados durante operações do NDMP.	Use esta classe de rastreio para depurar problemas nos comandos <b>BACKUP</b> e <b>RESTORE NODE</b> .
COLLOCATE	Esta classe de rastreio exibe informações sobre o processamento de disposição nos conjuntos de armazenamento. A classe de rastreio COLLOCATEDetail também pode ser usada para obter informações mais detalhadas sobre o processo de disposição. Por exemplo, informações sobre os arquivos que estão sendo processados para um grupo de disposição. Os arquivos que estão sendo processados para um grupo de disposição podem causar muitas instruções de rastreio de saída.	Use esta classe de rastreio para diagnosticar problemas com o processamento de disposição.
CRC	Esta classe de rastreio exibe informações sobre como gerar e gerenciar verificações de redundância cíclicas (CRCs) no servidor ou agente de armazenamento. CRC é uma classe de rastreio agregada que usa <b>CRCData</b> , <b>CRCProto</b> e <b>CRCVal</b> .	Use esta classe de rastreio para diagnosticar problemas de distorção de dados em que o processamento de CRC não relatou distorção de dados.

*Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)*

<b>Classes de Rastreio</b>	<b>descrição</b>	<b>Uso</b>
CRCDATA	Esta classe de rastreio exibe informações sobre como gerar e gerenciar CRCs para dados que são armazenados nos conjuntos de armazenamento com CRCDATA=YES configurado.	Use esta classe de rastreio para diagnosticar problemas de distorção de dados em que o processamento de CRC não relatou distorção de dados.
CRCPROTO	Esta classe de rastreio exibe informações sobre como gerar e gerenciar CRCs para dados que são trocados entre o cliente e o servidor ou agente de armazenamento no qual esse nó está configurado com VALIDATEPROTOCOL=ALL ou VALIDATEPROTOCOL=DATAOnly no servidor.	Use esta classe de rastreio para diagnosticar problemas de distorção de dados em que o processamento de CRC não relatou distorção de dados.
CRCVAL	Esta classe de rastreio exibe informações sobre como gerar e comparar valores de CRC.	Informações mostrando os valores de CRC durante o processamento.
CRYPTO	Esta classe de rastreio exibe informações sobre operações de Padrão de Criptografia Avançado (AES) e algumas configurações de criptografia gerais.	Use essa classe de rastreio para isolar e identificar problemas relacionados à criptografia.
DBCLI	Rastreia o conjunto geral de interações.	Use esta classe de rastreio para rastrear o conjunto geral de interações do DB2 e a interface de linha de comandos do DB2.
DBCONN	Rastreia atividades da conexão.	Use esta classe de rastreio para rastrear conexões do IBM Spectrum Protect com conexões do DB2. Essa classe de rastreio mostra coisas, como a criação de identificadores de conexões e a designação de conexões à transações.
DBDBG	Rastreia processos de depuração. Você pode usar esta classe de rastreio primeiro quando estiver depurando um problema do banco de dados.	Use esta classe de rastreio para mostrar entrada ou saída da função, códigos de retorno de saída e as instruções que foram construídas e estão sendo executadas.

*Tabela 10. Classes de Rastreo do Servidor ou do Agente de Armazenamento (continuação)*

<b>Classes de Rastreo</b>	<b>descrição</b>	<b>Uso</b>
DBITXN	Rastreia atividades relacionadas à transação do banco de dados. As atividades relacionadas à transação dizem respeito à aquisição e liberação de travas na transação, à alocação e liberação de dbTxnDesc e ao processamento de confirmação de transação das funções da fase de preparação e confirmação.	Use esta classe de rastreo para rastrear atividades relacionadas à transação para a interface do banco de dados.
DBNETDB	Esta classe de rastreo exibe informações sobre operações sem LAN e a negociação e gerenciamento de informações entre o servidor e o agente de armazenamento.	Use esta classe de rastreo para diagnosticar problemas sem a LAN quando o servidor e o agente de armazenamento estão em níveis diferentes. Eles funcionam melhor quando estão no mesmo nível. Também é possível usar esta classe de rastreo para diagnosticar problemas com um agente de armazenamento que está obtendo informações de configuração do servidor.
DBRC	Rastreia os códigos de retorno a partir de funções no componente do banco de dados.	Use esta classe de rastreo para rastrear os códigos de retorno.
DEDUP	Rastreia o rastreo do caminho lógico geral para processamento de deduplicação de dados. Geralmente, não inclui caminhos de erro.	Use DEDUP para rastrear caminhos lógicos gerais para o processamento de deduplicação de dados.
DEDUP1	Rastreia caminhos de erro para processamento de deduplicação de dados.	Use DEDUP1 para rastrear caminhos de erros para o processamento de deduplicação de dados.
DEDUP2	Rastreia o caminho de impressão digital e de assinaturas digitais.	Use DEDUP2 para rastrear caminhos de assinatura digital e impressão digital.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
DELTA	Classe de rastreio para funções de grupo lógico. As classes de rastreio DELTA e GROUP são sinônimas.	Use esta classe de rastreio para depurar problemas com grupos lógicos, se grupos base delta (backup de subarquivo) ou grupos peer (Windows SYSTEM OBJECT ou backups de imagens). O processamento de grupo é relevante durante apenas qualquer operação que faça referência a objetos de backup. Os objetos de backup podem incluir backup e restauração do cliente, expiração, exclusão ( <b>DELETE FILESPACE</b> , <b>DELETE VOLUME</b> ), exportação/importação, geração e restauração do conjunto de backups, restauração sem consulta, auditoria do banco de dados e outros.
DF	Esta classe de rastreio exibe informações sobre dados do usuário que são armazenados em volumes de disco. DF é uma classe de rastreio agregada que ativa <b>DFCREATE</b> , <b>DFRTRV</b> , <b>DFMOVE</b> , <b>DFLOCK</b> , <b>DFTXN</b> e <b>DFCOPY</b> . Emita o comando <b>TRACE DISABLE DFLOCK</b> , a menos que as informações de bloqueio sejam explicitamente solicitadas ou necessárias.	Use esta classe de rastreio para diagnosticar problemas sobre leitura ou gravação de arquivos do usuário em volumes do disco.
DFCREATE	Esta classe de rastreio exibe informações sobre como armazenar dados do usuário em volumes do disco.	Use esta classe de rastreio para diagnosticar problemas ao gravar dados do usuário em volumes do disco.
DFMOVE	Esta classe de rastreio exibe operações que movem dados do usuário usando volumes do disco. As operações de movimentação são concluídas pelos processos do servidor MIGRATION, MOVE DATA e MOVE NODEDATA.	Use esta classe de rastreio para diagnosticar problemas com os processos do servidor de movimentação de dados.
DFRTRV	Esta classe de rastreio exibe informações sobre como ler dados do usuário de volumes do disco.	Use esta classe de rastreio para diagnosticar problemas ao ler dados do usuário a partir de volumes do disco.

Tabela 10. Classes de Rastreo do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreo	descrição	Uso
DS	Esta classe de rastreo exhibe informações sobre a seleção de volume, reserva de espaço, designação e gerenciamento de posicionamento de dados nos volumes do disco. DS é uma classe de rastreo agregada que ativa DSALLOC, DSRTRV, DSDEALLOC e DSVOL. Emita <b>TRACE</b> <b>DISABLE DSTXN</b> , a menos que as informações de bloqueio sejam explicitamente solicitadas ou necessárias.	Use esta classe de rastreo para diagnosticar muitos problemas diferentes sobre operações de leitura e gravação de dados de volume do disco.
DSALLOC	Esta classe de rastreo exhibe informações sobre como reservar e alocar espaços nos volumes de disco para o armazenamento de dados. O armazenamento de dados pode ser concluído em nome de uma sessão do cliente ou para operações de movimentação de dados do servidor, como <b>MIGRATION</b> , <b>MOVE DATA</b> ou <b>MOVE NODEDATA</b> .	Diagnostique problemas nos quais o servidor ou o agente de armazenamento relata que não há espaço disponível, mas parece ter espaço disponível na hierarquia de armazenamento.
DSDEALLOC	Esta classe de rastreo exhibe informações sobre como liberar e desalocar espaço nos volumes de disco. As operações de desalocação típicas no servidor são <b>EXPIRATION</b> , <b>MIGRATION</b> , <b>MOVE DATA</b> , <b>MOVE NODEDATA</b> , <b>AUDIT VOLUME</b> , <b>DELETE VOLUME</b> e <b>DELETE FILESPACE</b> .	Use esta classe de rastreo para diagnosticar problemas durante a exclusão de dados.
DSRTRV	Esta classe de rastreo exhibe informações sobre como ler dados dos volumes de disco.	Use esta classe de rastreo para diagnosticar problemas sobre leitura de dados, como <b>RESTORE</b> ou <b>RETRIEVE</b> client pelo cliente ou <b>MIGRATION</b> , <b>STORAGE POOL BACKUP</b> , <b>AUDIT VOLUME</b> , <b>GENERATE BACKUPSET</b> , <b>EXPORT</b> , <b>MOVE DATA</b> ou <b>MOVE NODEDATA</b> pelo servidor.
DSVOL	Esta classe de rastreo exhibe informações sobre a seleção e designação de volume para volumes do disco.	Use esta classe de rastreo para diagnosticar situações nas quais sessões ou processos estão aguardando volumes ou casos em que uma operação falha porque nenhum volume está disponível.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
ICVOLHST	Classe de rastreio para funções do histórico do volume.	Use esta classe de rastreio para depurar problemas com a criação de entradas no histórico do volume, por exemplo; durante <b>EXPORT</b> , <b>BACKUP DB</b> ou <b>GENERATE BACKUPSET</b> ) ou exclusão de entradas no histórico do volume, por exemplo, durante <b>DELETE VOLHISTORY</b> ).
IMFS	Classe de rastreio para funções de espaço no arquivo.	Use esta classe de rastreio para depurar problemas que estão relacionados a espaços no arquivo de inventário (por exemplo, durante <b>DELETE FILESPACE</b> ).
LANFREE	Esta classe de rastreio exibe informações gerais sobre operações sem LAN no servidor ou no agente de armazenamento. Além disso, ela mostra informações de erros das operações relacionadas às operações sem LAN. LANFREE é uma classe de rastreio agregada que ativa LNFVERB, LNFMEM, LNFENTRY e LNFDATA.	Qualquer falha sem a LAN.
MMS	Esta classe de rastreio exibe informações sobre bibliotecas de fitas e o servidor ou agente de armazenamento que usa essas bibliotecas. MMS é uma classe de rastreio agregada que ativa MMSBASE, MMSTXN, MMSLIB, MMSDRIVE, MMSOP, MMSMAN, MMSSCSI, MMSFLAG, MMSACSLs e MMSSHARE. Inclua as classes de rastreio NA e PVR quando estiver rastreando o MMS.	Usado para diagnosticar problemas com bibliotecas de fitas, inventários do volume de biblioteca ou outros problemas gerais da biblioteca.
MONITOR	Esta classe de rastreio exibe informações sobre o monitoramento de alertas.	Use esta classe de rastreio para determinar por que um alerta não pode ser gerado.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
NA	Esta classe de rastreio exibe informações sobre o caminho do servidor ou agente de armazenamento. Estas informações estão relacionadas aos comandos <b>DEFINE PATH</b> , <b>UPDATE PATH</b> , <b>DELETE PATH</b> e <b>QUERY PATH</b> . Esta classe de rastreio também é usada para identificar problemas que estão relacionados a operações que envolvem servidores de arquivos NDMP, por exemplo comandos <b>DEFINE DATAMOVER</b> , <b>UPDATE DATAMOVER</b> , <b>BACKUP NODE</b> e <b>RESTORE NODE</b> . Esta classe de rastreio agregada usa NALOCK, NAPATH, NAMOVER, NADISK e NACONFIG. Pode ser melhor incluir as classes de rastreio MMS e PVR durante o rastreio de NA.	Use esta classe de rastreio para diagnosticar problemas com caminhos para dispositivos.
PRODCONS	Se houver problemas para despachar o trabalho para lotes, PRODCONS exibirá informações sobre o problema e se ele está no objeto PC ou na replicação.	Use PRODCONS para rastrear os trabalhos internos dos objetos do produtor/consumidores que são usados no servidor.
PROXYNODE	Esta classe de rastreio exibe informações sobre sessões de proxynode e os comandos que estão relacionados às associações de proxynode (GRANT, REVOKE, QUERY PROXYNODE).	Use esta classe de rastreio para diagnosticar problemas com sessões de nó do proxy e comandos relacionados. Pode ser melhor incluir o rastreio de SESSION durante a análise de problemas da sessão de proxynode.
PVR	Esta classe de rastreio exibe informações sobre o uso de dispositivos de mídias sequenciais e do servidor ou do agente de armazenamento desses dispositivos. PVR é uma classe de rastreio agregada que ativa PVRVOL, PVRCLASS e PVRMP.  A classe de rastreio PVR contém tudo na classe de rastreio agregada PVRIO e na classe de rastreio PVRNOIO.	Use esta classe de rastreio para diagnosticar problemas com unidades de fita, falhas ao ler ou gravar volumes da fita ou outros problemas relacionados ao volume da fita.



*Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)*

<b>Classes de Rastreio</b>	<b>descrição</b>	<b>Uso</b>
PVRIO	Esta classe de rastreio exhibe o rastreio das operações de leitura, gravação ou POS do uso de dispositivos de mídias sequenciais ou do servidor ou agente de armazenamento desses dispositivos.	Use esta classe de rastreio para diagnosticar problemas com falhas de unidade de fita ao ler ou gravar volumes da fita.
PVRNOIO	Esta classe de rastreio exhibe as informações PVRVOL, PVRCLASS e PVRMP.	Use esta classe de rastreio para diagnosticar problemas com conjuntos de unidades de fitas ou outros problemas relacionados ao volume de fita.
REPL	REPL é uma classe de rastreio agregada que ativa REPLBATCH, REPLCMD, REPLFS, REPLINV, REPLPROC, REPLSTATS e REPLSESS.	Use esta classe de rastreio para diagnosticar problemas com a replicação.
REPLBATCH	Esta classe de rastreio exhibe o rastreio relacionado ao processamento em lote, no qual arquivos individuais são enviados do servidor de origem para o servidor de destino.	Use esta classe de rastreio para diagnosticar problemas de replicação com o processamento em lote.
REPLCMD	Esta classe de rastreio exhibe o rastreio relacionado à análise de comando e resolução de regras de replicação de espaço no arquivo.	Use esta classe de rastreio para diagnosticar problemas de replicação com a análise de comando e a resolução de regras de replicação de espaço no arquivo.
REPLFS	Esta classe de rastreio exhibe o rastreio relacionado à iteração de espaços no arquivo para decidir o que será replicado, atualizado ou excluído.	Use esta classe de rastreio para diagnosticar problemas de replicação com os espaços no arquivo em iteração para decidir o que será replicado, atualizado ou excluído.
REPLINV	Esta classe de rastreio exhibe o rastreio relacionado às atualizações de inventário (tabelas IM) como parte da replicação.	Use esta classe de rastreio para diagnosticar problemas de replicação com atualizações do inventário.
REPLPROC	Esta classe de rastreio exhibe o rastreio de todo o processo de replicação. Esta classe de rastreio é o encadeamento e dispatcher principais.	Use esta classe de rastreio para diagnosticar problemas de replicação com o processo de replicação.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
REPLSESS	Esta classe de rastreio exibe o rastreio relacionado ao estabelecimento de sessões para replicação, incluindo o gerenciamento de sessões dos servidores de origem e destino.	Use esta classe de rastreio para diagnosticar problemas de replicação com o estabelecimento de sessões.
REPLSTATS	Esta classe de rastreio exibe o rastreio relacionado à atualização de estatísticas à medida que a replicação é executada. Também inclui a inserção ou atualização de registros de históricos na tabela de histórico de replicação.	Use esta classe de rastreio para diagnosticar problemas de replicação com atualizações estatísticas.
RETPROT	Classe de rastreio para as funções de proteção de retenção de archive.	Use esta classe de rastreio para depurar problemas durante o uso dos parâmetros <b>RETINIT</b> e <b>RETMIN</b> no grupo de cópias de archive. Também é possível usar esta classe de rastreio para problemas causados pelo uso do verbo VB_SignalObject (suportado somente pela API do cliente) para sinalizar um evento de objeto ou para suspender ou liberar um objeto. Por último, é possível usar esta classe de rastreio para problemas durante a expiração ou exclusão de objetos protegidos por retenção.
ROWMGR	Rastreia atividades para operações baseadas em linha. As operações baseadas em linha são as seguintes: <ul style="list-style-type: none"> <li>• Abbrev</li> <li>• Excluir</li> <li>• Fetch</li> <li>• FetchNext</li> <li>• FetchPrev</li> <li>• Insert</li> <li>• SearchBounds</li> <li>• Update</li> </ul>	Use esta classe de rastreio para rastrear as atividades para operações baseadas em linha.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
SCHED	Classe de rastreio para funções do planejador central. Esta classe de rastreio se aplica igualmente a planejamentos clássicos e aprimorados.	Use esta classe de rastreio para depurar problemas que estão relacionados a comandos de planejamento, como <b>DEFINE/UPDATE/QUERY SCHEDULE</b> ou <b>DEFINE ASSOCIATION</b> . Também use esta classe de rastreio para depurar problemas que estão relacionados a processos de segundo plano do planejador central, como o gerenciador de planejamento e o solicitante de planejamento.
SESSION	Esta classe de rastreio exibe informações sobre as sessões que estão conectadas ao servidor, incluindo todos os verbos que são enviados e recebidos pelo servidor.	Esta classe de rastreio é usada para violações de protocolo, erros de processamento de transações, ou nos casos em que o cliente é interrompido e não está respondendo.
SESSREMOTE	Rastreia a comunicação entre o servidor e o cliente durante operações de backup e restauração de NDMP.	Esta classe de rastreio é usada para identificar operações de backup ou restauração relacionadas ao NDMP que são iniciadas durante o uso do cliente da web ou da linha de comandos do IBM Spectrum Protect.
SHRED	Esta classe de rastreio exibe informações que estão relacionadas a operações de fragmentação de dados no servidor.	Esta classe de rastreio é usada para diagnosticar problemas com a fragmentação de dados. A fragmentação de dados será aplicável somente se um ou mais conjuntos de armazenamentos no servidor tiverem um valor diferente de zero para o atributo SHRED. A atividade que está relacionada à fragmentação de dados ocorre principalmente durante os comandos <b>EXPIRE INVENTORY</b> , <b>DELETE FILESPACE</b> , <b>DELETE VOLUME</b> , <b>MOVE DATA</b> , <b>MIGRATE</b> e <b>SHRED DATA</b> . Outras classes de rastreio que relatam a atividade relacionada à fragmentação de dados são <b>BFDESTROY</b> , <b>DFDESTROY</b> , <b>DSALLOC</b> , <b>DSDEALLOC</b> e <b>CRCDATA</b> .

*Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)*

<b>Classes de Rastreio</b>	<b>descrição</b>	<b>Uso</b>
SPI/SPID	Rastreia a interface de protocolo NDMP do servidor.	As classes de rastreio SPI e SPID são usadas para identificar problemas que estão relacionados a operações de backup ou restauração do NDMP de servidores de arquivos NAS. Estas classes de rastreio são específicas das funções que implementam o protocolo NDMP e se comunicam com um servidor de arquivos NAS. A classe de rastreio SPID fornece rastreio mais detalhado, incluindo o rastreio de todos os registros de histórico do arquivo NDMP que são enviados pelo servidor de arquivos NAS.
SSLDATA	O rastreio detalhado de Secure Sockets Layer (SSL) é usado para exibir informações em nível de byte sobre dados enviados ou recebidos entre o cliente de backup-archive e o servidor.	Use a classe de rastreio SSLDATA para depurar problemas de distorção de dados da sessão que podem ser causados pelo SSL que está em execução através das opções do servidor SSLTCP ou SSLTCPADMIN. Este rastreio é um rastreio em nível de byte, portanto, ele pode coletar uma grande quantidade de dados.
SSLINFO	O rastreio geral de SSL é usado para exibir configuração e características de sessões SSL entre o cliente de backup-archive e o servidor.	Use a classe de rastreio SSLINFO para depurar erros de conexão da sessão e de handshake que podem ser causados pelo SSL que está em execução através das opções do servidor SSLTCP ou SSLTCPADMIN. Esta classe de rastreio pode ser usada juntamente com as classes de rastreio TCPINFO e SESSION.
TBREORG	Esta classe de rastreio coleta informações sobre atividades de reorganização de tabelas e de índices que são iniciadas pelo servidor.	Use a classe de rastreio TBREORG para depurar a atividade de reorganização iniciada pelo servidor.
TBLMGR	Rastreia atividades para operações baseadas em tabela.	Use a classe de rastreio TBLMGR para visualizar operações baseadas em tabela, tais como, registro de tabela, abertura de tabela e fechamento de tabela.

*Tabela 10. Classes de Rastreo do Servidor ou do Agente de Armazenamento (continuação)*

Classes de Rastreo	descrição	Uso
TCP	Esta classe de rastreo coleta informações sobre o TCP/IP usado entre o cliente e o servidor ou agente de armazenamento. TCP é uma classe de rastreo agregada. Ativa TCPINFO e TCPERROR.	Use esta classe de rastreo para depurar erros de conexão ou de distorção de dados da sessão que podem ser causados pela rede.
TCPDATA	O rastreo detalhado de TCP/IP é usado para exibir informações em nível de byte sobre dados que são enviados ou recebidos.	Use esta classe de rastreo para depurar problemas de distorção de dados da sessão que podem ser causados pela rede.
TCPINFO	O rastreo geral de TCP/IP é usado para exibir a configuração e características do TCP/IP no servidor ou agente de armazenamento.	Use esta classe de rastreo para depurar problemas de distorção de dados da sessão que podem ser causados pela rede.
TEC	Esta classe de rastreo fornece informações sobre eventos que são enviados para um servidor TEC. Esses eventos correspondem ao receptor de eventos TIVOLI.	Para depurar problemas de conexão incorridos pela criação de log de eventos do TEC.
TOC	Esta classe de rastreo é usada para o componente Índice (TOC), que é usado durante operações de NDMP em nível de arquivo. TOC é uma classe de rastreo agregada que ativa TOCBUILD, TOCLOAD, TOCREAD e TOCUTIL.	Use esta classe de rastreo para depurar problemas durante operações NDMP em nível de arquivo, tais como backup NDMP com o parâmetro TOC=YES ou uma restauração NDMP com o parâmetro <b>FILELIST</b> .
TOCBUILD	Funções de construção de Índice (TOC).	Use esta classe de rastreo para depurar problemas durante um backup NDMP com o parâmetro <b>TOC=YES</b> .
TOCLOAD	Funções de carregamento de Índice (TOC).	Use esta classe de rastreo para depurar problemas durante a exibição de arquivos e diretórios na interface gráfica com o usuário (GUI) do cliente.
TOCREAD	Funções de leitura de Índice (TOC).	Use esta classe de rastreo para depurar problemas durante um comando <b>QUERY TOC</b> ou quando estiver tentando carregar um TOC para exibir arquivos e diretórios na GUI do cliente.

Tabela 10. Classes de Rastreio do Servidor ou do Agente de Armazenamento (continuação)

Classes de Rastreio	descrição	Uso
TOCUTIL	Funções de utilitário de Índice (TOC).	Use esta classe de rastreio para depurar problemas que estão relacionados à inicialização do componente TOC ou à retenção do TOC.
UNICODE	Esta classe de rastreio exibe informações sobre as conversões da página de código e as operações de espaço no arquivo Unicode.	Use esta classe de rastreio para depurar problemas que estão relacionados a problemas de conversão de página de códigos ou problemas de espaço no arquivo Unicode.
XI	Esta classe de rastreio exibe informações gerais para os comandos <b>IMPORT</b> e <b>EXPORT</b> .	Use esta classe de rastreio para depurar problemas que estão relacionados aos comandos <b>IMPORT</b> e <b>EXPORT</b> .

## Comandos Show para o Servidor e o Agente de Armazenamento

Os comandos **SHOW** são comandos de diagnóstico não suportados que são usados para mostrar informações sobre estruturas de controle de memória e outros atributos de tempo de execução. Os comandos **SHOW** são usados pelo desenvolvimento e serviço apenas como ferramentas de diagnóstico. Existem vários comandos **SHOW** para o cliente de backup-archive.

Dependendo das informações que um comando **SHOW** mostra, pode haver situações em que as informações estão sendo alteradas ou casos em que elas podem causar a parada do aplicativo (cliente, servidor ou agente de armazenamento). Os comandos **SHOW** devem ser usados apenas com a recomendação do Suporte de Software IBM. Os comandos **SHOW** que estão incluídos aqui fazem parte dos comandos **SHOW** disponíveis.

Tabela 11. Comandos SHOW do Servidor ou do Agente de Armazenamento

Comando SHOW	Descrição	Recomendação
AGGREGATE	Mostra informações sobre um objeto agregado na hierarquia de armazenamento do servidor. A sintaxe é <b>SHOW AGGRegate aggrID-high aggrID-low. aggrID-high e aggrID-low</b> são as palavras de 32 bits de alta ordem e de baixa ordens do ID agregado de 64 bits do agregado que está sendo consultado.	Emita este comando para determinar a existência e arquivos lógicos que estão armazenados em um objeto agregado na hierarquia de armazenamento do servidor. O deslocamento, comprimento e estado ativo do arquivos de backup são exibidos para arquivos no agregado. Se tiver problemas ao restaurar ou recuperar arquivos, expirar ou mover dados, fazer backup de conjuntos de armazenamentos primários, copiar dados ativos para data conjuntos de dados ou auditar volumes, você pode emitir este comando.

Tabela 11. Comandos *SHOW* do Servidor ou do Agente de Armazenamento (continuação)

Comando <i>SHOW</i>	Descrição	Recomendação
ASQUEUED	Mostra a fila de ponto de montagem. A sintaxe é <b>SHOW ASQueued</b> .	Para usar uma unidade, uma sessão do cliente ou processo do servidor, primeiro você deve obter um ponto de montagem. O gerenciamento do ponto de montagem no servidor permite o enfileiramento de tarefas em espera para pontos de montagem, se forem necessários mais pontos de montagem do que os que estão disponíveis. Este comando é útil para determinar o estado de uma solicitação de ponto de montagem, principalmente se uma sessão ou processo estiver interrompido e aguardando um ponto de montagem.
ASVOL	Mostra volumes designados. A sintaxe é <b>SHOW ASVol</b> .	Como os volumes de mídia sequencial são designados para uso por uma sessão ou processo, eles são rastreados em uma lista de memória. É possível visualizar esta lista para determinar o estado de volumes em uso, e situações de paradas ou conflito nas quais uma sessão ou processo está interrompido, aguardando um volume ou retendo um volume e aguardando algo mais.
BFOBJECT	Mostra as seguintes informações nos dados da hierarquia de armazenamento do servidor: <ul style="list-style-type: none"> <li>• O estado ativo/inativo de arquivos lógicos em um agregado</li> <li>• O deslocamento/comprimento de arquivos lógicos em um agregado</li> <li>• O estado ativo ou ID do arquivo de bits do proprietário de arquivos lógicos em um agregado</li> <li>• O ID do arquivo de bits do link se a extensão deduplicada estiver vinculada à outra extensão</li> </ul> A sintaxe é <b>SHOW BFObject</b> .	Este comando ajuda a determinar a existência e atributos de um objeto do arquivo de bits na hierarquia de armazenamento do servidor. Se tiver problemas ao restaurar, recuperar, expirar ou auditar o objeto, você pode emitir este comando.

Tabela 11. Comandos SHOW do Servidor ou do Agente de Armazenamento (continuação)

Comando SHOW	Descrição	Recomendação
CMD DEDUPDELETEINFO	Mostra o status de encadeamentos de exclusão secundários para objetos desreferenciados ou deduplicados.	Emita esse comando para verificar o status do processo de exclusão de plano de fundo de objetos deduplicados. Quando um arquivo é excluído ou movido para fora de um conjunto de armazenamento deduplicado, as extensões são enfileiradas para um processador de plano de fundo para tentativas de remoção do conjunto de armazenamento. Esse comando é útil para a verificação da lista não processada de extensões enfileiradas e do status de cada encadeamento de exclusão.
CONFIGURATION	O comando <b>CONFIGURATION</b> é um comando SHOW de resumo que, de fato, emite muitos comandos show diferentes e consultas. A sintaxe é <b>SHOW CONFIGuration</b> .	Emita esse comando para fornecer configuração geral e outras informações sobre o servidor para o serviço IBM.
DB2CONNECTIONS	O comando DB2CONNECTIONS mostra as conexões do DB2 definidas a partir de diversos conjuntos de conexões. Este comando não requer nenhum parâmetro adicional. A sintaxe é <b>SHOW DB2CONnections</b> .	Emita este comando para mostrar quantas conexões do DB2 estão definidas, em uso e livres, no total e em um conjunto específico.
DB2TABLES	O comando DB2TABLES mostra as tabelas registradas e seus atributos de coluna. Este comando não requer nenhum parâmetro adicional. A sintaxe é <b>SHOW DB2TABles</b> .	Emita este comando para mostrar as tabelas registradas e seus atributos de coluna.
DBVARS	Mostra os atributos globais do banco de dados. A sintaxe é <b>SHOW DBVars</b> .	Emita este comando para visualizar o estado atual e atributos do banco de dados do servidor.



Tabela 11. Comandos *SHOW* do Servidor ou do Agente de Armazenamento (continuação)

Comando <i>SHOW</i>	Descrição	Recomendação
DEDUPOBJECT	Mostra informações de deduplicação de dados para arquivos. Ao emitir esse comando, é necessário especificar o parâmetro <b>objectID</b> . Emita o comando <b>SHOW VERSION</b> para determinar o valor desse parâmetro. A sintaxe é <b>SHOW DEDUPObject</b> .	Emita este comando para mostrar informações de deduplicação de dados, tais como: <ul style="list-style-type: none"> <li>• O ID do arquivo de bits para cada extensão</li> <li>• O ID do arquivo de bits de propriedade</li> <li>• O deslocamento e comprimento do arquivo de bits de propriedade</li> <li>• O tipo e valor de compilação do objeto de deduplicação de dados</li> </ul>
DEVCLASS	Mostra informações sobre classes de dispositivo. A sintaxe para este comando é <b>SHOW DEVClass</b> .	Emita este comando para mostrar os estados de unidades alocadas, atributos da classe de dispositivo e outras informações. Este comando geralmente é usado para diagnosticar problemas com dispositivos ou bloqueios que estão aguardando uma unidade, biblioteca ou volume. O comando <b>SHOW LIBRARY</b> também fornece informações complementares válidas sobre unidades e bibliotecas.
GROUPLEADERS	Mostra todos os líderes do grupo de backup de um objeto no inventário do servidor. A sintaxe é <b>SHOW GROUPLeaders objID-high objID-low</b> . <i>objID-high</i> e <i>objID-low</i> são as palavras de 32 bits de alta ordem e de baixa ordem do ID do objeto de 64 bits do objeto que está sendo consultado. A palavra alta ordem é opcional; se não for especificada, será assumido um valor zero. O objeto deve ser um objeto de backup.	Emita este comando para determinar os relacionamentos do grupo de backup de um objeto no inventário do servidor. Se tiver problemas ao restaurar, recuperar, expirar ou auditar o objeto, você pode emitir este comando.

Tabela 11. Comandos *SHOW* do Servidor ou do Agente de Armazenamento (continuação)

Comando <i>SHOW</i>	Descrição	Recomendação
GROUPMEMBERS	Mostra todos os membros do grupo de backup de um objeto no inventário do servidor. A sintaxe é <b>SHOW GROUPMembers</b> <i>objID-high objID-low. objID-high e objID-low</i> são as palavras de 32 bits de alta ordem e de baixa ordem do ID do objeto de 64 bits do objeto que está sendo consultado. A palavra alta ordem é opcional; se não for especificada, será assumido um valor zero. O objeto deve ser um objeto de backup.	Emita este comando para determinar os relacionamentos do grupo de backup de um objeto no inventário do servidor. Se tiver problemas ao restaurar, recuperar, expirar ou auditar o objeto, você pode emitir este comando.
INVOBJECT	Mostra informações sobre um objeto do inventário no servidor. A sintaxe é <b>SHOW INVOBJECT</b> <i>objID-high objID-low. objID-high e objID-low</i> são as palavras de 32 bits de alta ordem e de baixa ordem do ID do objeto de 64 bits do objeto que está sendo consultado. A palavra alta ordem é opcional; se não for especificada, será assumido um valor zero. O objeto pode ser um objeto de backup, um objeto de archive, um objeto gerenciado por espaço e outros.	Emita esse comando para determinar a existência e os atributos de um objeto no inventário do servidor. É possível emitir este comando se você estiver com problemas ao restaurar, recuperar, expirar ou auditar o objeto.  O comando <b>INVOBJECT</b> relata os seguintes itens: <ul style="list-style-type: none"> <li>• Novas informações para os objetos protegidos por retenção de archive.</li> <li>• Se o objeto de archive está com exclusão suspensa.</li> <li>• Se o objeto usa a retenção baseada em eventos.</li> </ul>
LIBINVENTORY	Mostra o estado atual do inventário de biblioteca para a biblioteca especificada. A sintaxe é <b>SHOW LIBINVENTORY</b> <i>libraryName</i> , em que <i>libraryName</i> é opcional, e se for removido, o comando retornará as informações sobre o inventário para todas as bibliotecas.	Emita este comando se houver um problema com as informações sobre o inventário da biblioteca. O comando mostra as propriedades de memória atual do inventário de biblioteca.
BIBLIOTECA	Use o comando <b>LIBRARY</b> para mostrar o estado atual da biblioteca especificada e todas as suas unidades. A sintaxe é <b>SHOW LIBRARY</b> <i>libraryName</i> , em que <i>libraryName</i> é opcional. Se for removido, o comando retornará informações para todas as bibliotecas.	Este comando é útil para reunir uma visualização rápida de todas as informações de memória sobre uma biblioteca e suas unidades. Esta saída pode ser reunida para qualquer problema relacionado a bibliotecas ou unidades; por exemplo, problemas de montagem.

Tabela 11. Comandos SHOW do Servidor ou do Agente de Armazenamento (continuação)

Comando SHOW	Descrição	Recomendação
LOCK	Mostra portadores e esperas de bloqueio. A sintaxe é <b>SHOW LOCK</b> .	O servidor e o agente de armazenamento usam bloqueios como um mecanismo para serializar o acesso e atualizações para informações e outras construções. Estas informações são usadas para diagnosticar interrupções ou outros problemas de contenção de recursos.
MEMTREND	O comando <b>MEMTREND</b> relata a memória que é usada pelo servidor, em megabytes. É registrado em intervalos por hora para as últimas 50 horas. Este comando está configurado no código do servidor. Isso não é configurável. O comando também mostra um histograma para ajudar a visualizar a tendência de uso. A sintaxe é <b>SHOW MEMTREnd</b> .	Emita este comando para determinar se o servidor possui uma fuga de memória. Se o uso da memória estiver aumentando constantemente, pode ter ocorrido uma fuga de memória. Para que as medições sejam válidas, o período de medição (as últimas 50 horas) deve ser atividade do servidor de estado normal, estável. O uso relatado representa a quantidade de memória que as rotinas do servidor internas solicitam das rotinas de memória de pseudokernel. Ele NÃO representa a quantidade total de memória que o servidor está usando. Este comando ajuda a determinar a tendência de uso da memória do servidor.
MP	Mostra pontos de montagem. A sintaxe é <b>SHOW MP</b> .	Emita este comando para determinar qual volume está em uso por um ponto de montagem e outros atributos para os pontos de montagem designados. <b>SHOW LIBRARY</b> e <b>SHOW DEVCLASS</b> possuem informações complementares úteis com esse comando para mostrar o estado atual de unidades e de contagens de pontos de montagem devclass atuais.
NASDEV	Mostra os dispositivos SCSI que estão conectados a um servidor de arquivos de armazenamento conectado à rede (NAS) que está associado a uma definição de movedor de dados do NAS. A sintaxe é <b>SHOW NASDev</b> .	Crie uma conexão de Protocolo de Gerenciamento de Dados de Rede (NDMP) para o servidor de arquivos NAS especificado e mostre os dispositivos SCSI conectados no servidor de arquivos. Este comando requer apenas um nó e uma definição de movedor de dados do NAS.

Tabela 11. Comandos SHOW do Servidor ou do Agente de Armazenamento (continuação)

Comando SHOW	Descrição	Recomendação
NASFS	Mostra os sistemas de arquivos em um servidor de arquivos NAS que está associado a uma definição de movedor de dados do NAS. A sintaxe é <b>SHOW NASFSs</b> .	Crie uma conexão NDMP com o servidor de arquivos NAS especificado e mostre os sistemas de arquivos que estão definidos no servidor de arquivos. Os sistemas de arquivos mostrados podem receber backup pelo IBM Spectrum Protect. Este comando requer apenas um nó e uma definição de movedor de dados do NAS.
NASINFORMATION	Mostra informações de configuração sobre o servidor de arquivos NAS que está associado a uma definição de movedor de dados do NAS. A sintaxe é <b>SHOW NASInformation</b> .	Crie uma conexão NDMP com o servidor de arquivos NAS especificado e mostre as informações de configuração gerais recuperadas do servidor de arquivos. Este comando é útil para identificar problemas de comunicação básicos com servidores de arquivos NAS, tais como erros de autenticação. Este comando requer apenas um nó e uma definição de movedor de dados do NAS.
NASWORKLOAD	Mostra a carga de trabalho de arquivos NAS que são usados para todas as operações do IBM Spectrum Protect. A sintaxe é <b>SHOW NASWorkload</b> .	Emita este comando para determinar a carga de trabalho de operações de backup e restauração e movimentação de dados de backend.
REPLICATION	Mostra todos os servidores de replicação conhecidos e seus identificadores exclusivos globais (GUID) e todos os processos de replicação em execução. Os processos podem incluir as estatísticas individuais de cada espaço de arquivo e o status de cada sessão de replicação.	Emita este comando se a replicação não estiver progredindo ou se não estiver funcionando corretamente.
RESQUEUE	Mostra a fila de recursos. A sintaxe é <b>SHOW RESQueue</b> .	Use a fila de recursos para monitorar recursos comuns no servidor. Se um recurso estiver interrompido ou retendo um recurso por um período de tempo excessivo, os algoritmos de monitoramento de recursos para o servidor cancelarão o usuário do recurso. Este comando é usado para mostrar informações sobre transações, bloqueios e outros recursos que são usados por um agente de armazenamento no servidor de banco de dados que ele está configurado para usar.

Tabela 11. Comandos *SHOW* do Servidor ou do Agente de Armazenamento (continuação)

Comando <b>SHOW</b>	Descrição	Recomendação
SESSIONS	Mostra informações sobre sessões que estão conectadas ao servidor ou ao agente de armazenamento. A sintaxe é <b>SHOW SESSIONS</b> .	Emita este comando para diagnosticar interrupções ou outros problemas gerais de sessão enquanto uma sessão ainda está conectada ao servidor. Este comando também é útil nos casos em que uma sessão é cancelada e ainda está sendo mostrada em <b>QUERY SESSION</b> .
SLOTS	Mostra o estado atual das informações de slot da biblioteca especificada; por exemplo, quais volumes estão na biblioteca e em qual slot). A sintaxe é <b>SHOW SLOTS libraryName</b> .	As informações mostradas são as informações salvas diretamente do hardware da biblioteca para valores de memória. Essas informações podem ser usadas para determinar se estas informações estão fora de sincronização, incorretas ou se os valores retornados do próprio hardware da biblioteca estão incorretos.  Como alternativa, emita este comando para determinar os números de elementos da unidade para uma biblioteca SCSI, se <b>QUERY SAN</b> estiver indisponível para uma determinada biblioteca.
SSPOOL	Mostra informações de conjuntos de armazenamentos. A sintaxe é <b>SHOW SSPool</b> .	Emita este comando para mostrar os estados e atributos de conjuntos de armazenamentos definidos.

Tabela 11. Comandos SHOW do Servidor ou do Agente de Armazenamento (continuação)

Comando SHOW	Descrição	Recomendação
THREADS	<p>Mostra informações sobre todos os encadeamentos que são conhecidos no servidor. A sintaxe é <b>SHOW THReads</b>.</p> <p><b>Importante:</b> Em alguns sistemas operacionais (como um exemplo: HP), as informações que são relatadas são obtidas sem serialização. Em um sistema ocupado, as informações podem ser inconsistentes, vários encadeamentos podem relatar a retenção do mesmo mutex, ou um encadeamento pode relatar que está aguardando um mutex que está retido por outro encadeamento que não reivindica sua retenção.</p>	<p>O servidor exibe informações sobre cada encadeamento, geralmente incluindo o ID do encadeamento do IBM Spectrum Protect, o ID do encadeamento do sistema, o nome do encadeamento, os mutexes que ele suspende (se houver algum) e o mutex ou condição que ele está aguardando (se houver algum). Este comando é específico da plataforma, portanto, cada plataforma pode ter informações um pouco diferentes. Talvez você queira emitir este comando, se o servidor ou um determinado processo do servidor for interrompido para que seja possível ver se há encadeamentos aguardando recursos retidos por outro encadeamento.</p>
TOCSETS	<p>Mostra todos os conjuntos do Índice (TOC) conhecidos no servidor. A sintaxe é <b>SHOW TOCSETS DELETE=setNum TOUCH=setNum</b>. O parâmetro <b>DELETE</b> faz o número do conjunto do TOC especificado ser excluído. O parâmetro <b>TOUCH</b> atualiza a data da última utilização do número do conjunto do TOC especificado. Um conjunto do TOC é retido durante o período de retenção do TOC que segue a data do último uso (consulte o comando <b>SET TOCRETENTION</b>).</p>	<p>Um conjunto do TOC é usado durante operações NDMP em nível do arquivo. Durante um backup do NDMP com o parâmetro TOC=YES, é construído um TOC no banco de dados do servidor. Durante uma restauração, um ou mais TOCs podem ser carregados no banco de dados do servidor para fornecer nomes de arquivos e diretórios à GUI do cliente. Este comando mostra o status do conjunto do TOC; por exemplo, construção ou carregamento, e a quantidade de espaço de banco de dados temporário que está em uso para cada conjunto do TOC. Você pode emitir esse comando se estiver com problemas em um backup de NDMP com o parâmetro <b>TOC=YES</b> ou tiver problemas para restaurar arquivos de um backup NDMP ou se os conjuntos TOC estiverem sendo retidos no banco de dados do servidor por muito tempo ou por tempo não suficiente.</p>

Tabela 11. Comandos *SHOW* do Servidor ou do Agente de Armazenamento (continuação)

Comando <i>SHOW</i>	Descrição	Recomendação
TOCVARS	Mostra informações sobre o componente TOC do servidor. A sintaxe é <b>SHOW TOCVars</b> .	Emita este comando para determinar o status do componente TOC. Você pode emitir este comando se estiver tendo problemas ao concluir um backup de NDMP com o parâmetro <b>TOC=YES</b> , ou se tiver problemas ao restaurar arquivos de um backup de NDMP.
TXNTABLE	Mostra informações sobre transações que estão na lista em uso no servidor. A sintaxe é <b>SHOW TXNTable</b> .	As transações mineradas por este comando são usadas por processos do servidor, sessões ou outras operações para ler informações a partir do banco de dados, fazer atualizações no banco de dados (como inserir, atualizar ou excluir informações), ou para gerenciar bloqueios. Estas informações são úteis para diagnosticar interrupções ou outras falhas relacionadas à transação enquanto a transação ainda está aberta no servidor.
VALIDATE LANFREE	Valida se as definições estão prontas no servidor para que um cliente possa concluir operações de movimentação de dados sem LAN. Nos casos em que estas definições não estão presentes ou estão incorretas, pode ser difícil determinar se o ambiente sem a LAN está configurado corretamente. A sintaxe é <b>VALIDATE LANFREE nodeName storageAgent</b> . <b>Nota:</b> O comando <b>VALIDATE LANFREE</b> substituiu o comando <b>SHOW LANFREE</b> .	Este comando avalia todos os possíveis conjuntos de armazenamentos de destino para este nó cliente e relata se o conjunto de armazenamentos suporta operações de movimentação de dados sem LAN.
VERSIONS	Emita o comando <b>SHOW VERSIONS</b> para recuperar um <b>objectID</b> . O <b>objectID</b> é necessário para emitir o comando <b>SHOW DEDUPOBJECT</b> . A sintaxe é <b>SHOW Versions</b> .	Emita este comando para mostrar os IDs de objeto.

Tabela 11. Comandos SHOW do Servidor ou do Agente de Armazenamento (continuação)

Comando SHOW	Descrição	Recomendação
VOLINUSE	Mostra se o volume especificado está na lista em uso do servidor. O comando <b>VOLINUSE</b> mostra informações extras que podem ser úteis, incluindo se o volume está com remoção pendente na lista em uso. A sintaxe é <b>SHOW VOLINUSE volumeName</b> . Se o volume precisar ser removido da lista em uso, será possível especificar o seguinte parâmetro para remover o volume da lista: <b>SHOW VOLINUSE volumeName REMOVE=YES</b> .	Emita este comando para determinar se um volume está na lista em uso e, se necessário, para removê-lo dessa lista. As operações que estão associadas a este volume poderão falhar se o volume for removido da lista em uso.

## Ativando um Rastreo para o Driver de Dispositivo do IBM Spectrum Protect

O rastreo está disponível para o driver de dispositivo do IBM Spectrum Protect. O driver de dispositivo do IBM Spectrum Protect pode ser rastreado a partir do console do servidor, de um cliente administrativo ou de um shell em execução no sistema em que o driver de dispositivo está instalado.

As instruções de rastreo se aplicam ao driver de dispositivo do IBM Spectrum Protect em todas as plataformas nas quais o driver de dispositivo é suportado. Para dispositivos que usam drivers de dispositivo diferentes do driver de dispositivo do IBM Spectrum Protect, a capacidade de rastrear e instruções sobre como rastrear estes drivers de dispositivo são oferecidas pelo fornecedor do dispositivo.

### Referências relacionadas:

“Rastreo a partir do Console do Servidor”

“Rastreando dados a partir de um shell de comando para AIX e Windows” na página 152

## Rastreo a partir do Console do Servidor

Para rastrear o driver a partir do servidor, primeiro é necessário emitir os comandos apropriados.

Emita os comandos **TRACE ENABLE** e **TRACE BEGIN** para rastrear o driver a partir do servidor.

O driver de dispositivo do IBM Spectrum Protect realmente consiste em dois drivers: um para dispositivos de alterador de mídia de biblioteca e um para dispositivos de fita. É possível escolher o que você deseja rastrear. A seguinte sintaxe serve para o comando:

```
DDTRACE START [ LIBRARYDD | TAPEDD]
[flags=EE |, FULL |, SYSLOG | BASE ]
DDTRACE GET [ LIBRARYDD | TAPEDD]
DDTRACE END [ LIBRARYDD | TAPEDD]
```



As seguintes opções estão disponíveis:

**START** Ativa o rastreo e grava-o em um buffer da memória com base no padrão ou na opção **FLAGS** especificada.

**GET** Grava o buffer de memória no mesmo arquivo que foi especificado com o comando do servidor **TRACE BEGIN**.

**END** Para a gravação do rastreo no buffer de memória, mas não limpa o conteúdo do buffer, portanto, é possível executar **END** antes de executar **GET**.

#### **LIBRARYDD**

Rastreia o driver de dispositivo que controla os dispositivos de troca de biblioteca automáticos.

**TAPEDD** Rastreia o driver de dispositivo que controla unidades de fita.

Para as opções listadas acima, é possível especificar qualquer driver de dispositivo ou o driver de dispositivo de biblioteca e um dos outros dois. Eles são delimitados por espaço. Por Exemplo:

**DDTRACE START TAPEDD** - Inicia o rastreo do driver de dispositivo que controla unidades de fita.

**DDTRACE START LIBRARYDD** Iniciar o rastreo do dispositivo de troca de biblioteca automático.

**DDTRACE START LIBRARYDD TAPEDD** Rastreia as unidades de biblioteca e de fita.

Independentemente dos que forem usados, especifique os mesmos para todos os comandos na série start-get-end.

O parâmetro **FLAGS** é opcional e, geralmente, não é necessário. Os seguintes valores servem para o parâmetro **FLAGS**:

**EE** Rastreia todas as entradas e saídas da rotina do driver de dispositivo.

**FULL** Ativa mais rastreo de depuração e fornece mais detalhes. Como o tamanho do buffer de memória é fixo, no entanto, menos eventos são rastreados. Não rastreia entrada de rotina e pontos de saída.

#### **SYSLOG**

Em algumas plataformas, **SYSLOG** direciona as instruções de rastreo a serem gravadas no log do sistema, além do buffer da memória. Essa oferta é mais útil nas interrupções do kernel de depuração ou quando o rastreo é quebrado no buffer de memória.

**BASE** **BASE** é o padrão e não pode ser especificado com outros sinalizadores. É usado apenas para desativar os sinalizadores **EE**, **FULL** e **SYSLOG** sem desativar o rastreo.

## Rastreando dados a partir de um shell de comando para AIX e Windows

AIX

Windows

O utilitário independente, `ddtrace`, simula exatamente os comandos do servidor **DDTRACE**.

O utilitário `ddtrace` independente está instalado no diretório de dispositivos, que é o mesmo diretório dos utilitários `mttest`, `lbtest` e `optest`. Sua sintaxe e opções são idênticas ao comando do servidor **DDTRACE**. Por exemplo:

```
$ ddtrace start librarydd tapedd flags=EE - Começa a rastrear os drivers de biblioteca e de fita e obtém rastreo de entrada/saída adicional.
```

```
$ ddtrace get librarydd tapedd - Obtém o rastreo da memória e grava-o no arquivo ddtrace.out.
```

```
$ ddtrace end librarydd tapedd - Para o rastreo na memória.
```

O principal uso deste utilitário independente é especificamente para casos em que o driver precisa ser rastreado durante a inicialização do servidor IBM Spectrum Protect. O utilitário `ddtrace` grava o buffer de memória para o arquivo “`ddtrace.out`” no diretório atual. Se o arquivo existir, ele será anexado ao arquivo e não o sobrescreverá.

## Rastreio para Detectar uma Falha de Conversão de Página de Códigos

O servidor IBM Spectrum Protect usa funções do sistema operacional para converter entre Unicode e a página de códigos do servidor. Se o sistema não estiver configurado corretamente, a conversão falhará.

### Procedimento

Execute as seguintes etapas para obter informações adicionais sobre a falha:

1. Comece rastreando a classe de rastreo UNICODE.
2. Repita a ação que causou a mensagem de erro.
3. Verifique no arquivo LEIA-ME do servidor se existem requisitos específicos de plataforma para instalação de idioma.
4. Certifique-se de que os códigos do idioma indicados pelas páginas de códigos de problema estejam instalados e os requisitos listados no arquivo LEIA-ME estejam instalados.

---

## Dados de Rastreio para o Cliente

É possível ativar o rastreo no cliente ou na interface de programação de aplicativos (API) do cliente alterando o arquivo de opções do cliente.

### Sobre Esta Tarefa

Execute as seguintes etapas para ativar o rastreo no cliente ou na API do cliente:

## Procedimento

1. Determine as classes de rastreo a serem ativadas a partir da seguinte tabela:

Nome da Classe de Rastreo	Descrição	Quando utilizar	Notas Adicionais
SERVICE	Exibe informações gerais de processamento para o cliente.	Útil em muitos casos. Geralmente, é recomendado para violações de protocolo, erros de processamento de transações, ou nos casos em que o cliente é interrompido e não está respondendo.	
VERBINFO	Coleta informações relacionadas ao protocolo do cliente/servidor usado pelo IBM Spectrum Protect.	Para depurar violações de protocolo, erros de processamento de transações ou nos casos em que o cliente é interrompido e não está respondendo.	
VERBDETAIL	Informações detalhadas relacionadas ao protocolo do cliente/servidor usado pelo IBM Spectrum Protect. Exibe buffers de memória internos contendo os verbos enviados e recebidos pelo cliente.	Para depurar problemas de distorção de dados da sessão que podem ser causados pela rede.	Gera uma grande quantidade de saída.

2. Ative o rastreo incluindo o seguinte texto no arquivo de opções do cliente:  
`traceflag <nome da classe de rastreo>.`

**Atenção:** `<nome da classe de rastreo>` pode ser uma lista de classes de rastreo delimitada por vírgulas. Por exemplo, este texto pode ser inserido como  
`traceflag service,verbinfo,verbdetail.`

3. Configure o rastreo para ser iniciado e emita as mensagens de rastreo para um arquivo, incluindo o seguinte texto no arquivo de opções do cliente: `tracefile <nome do arquivo>.`

4. Execute a operação que está causando o problema.

**Dica:** O rastreo também pode ser configurado e iniciado invocando o cliente a partir de um prompt de comandos e especificando os sinalizadores acima. Por exemplo, `dsm -traceflags=service -tracefile=file.out.`

## Sinalizadores de Rastreio do Cliente e do Daemon de Diário

Para executar um backup baseado em diário, é necessário usar o processo Daemon de Diário. Este processo é usado para controlar mudanças no sistema de arquivos e manter os bancos de dados do diário de mudanças.

O Daemon de Diário usa o mesmo mecanismo de rastreio que o cliente, mas as configurações de rastreio são especificadas no arquivo de configuração de diário (tsmjbbd.ini), conforme a seguir:

```
[JournalSettings]
TraceFlags=all_jbb
;
; as duas configurações a seguir permitem a segmentação do arquivo de rastreio
;
TraceMax=100
TraceSegMax=1
tracefile=tracefiles\trace.out
```

Configurações de rastreio específicas do Daemon de Diário:

- BTREEDB - classe base do banco de dados BTREE de nível inferior
- CACHEDB - backup do cache de disco e processamento do cache de exclusão do Windows 2003
- DBPERF - desempenho da operação do banco de dados de nível inferior
- DBSTATS - rastreamento de desempenho de operações de consulta de banco de dados, inserção/atualização, exclusão e movimentação na árvore
- FILEOPS - atividade do banco de dados interna
- JBBCOMM - encadeamento de atendimento
- JBBDAEMON - gerenciador de processos
- JBBFILEMON - monitor do sistema de arquivos
- JBBDBACCESS - encadeamento do controlador do banco de dados
- JBBDBINFO - acesso ao banco de dados de nível inferior
- JBBNPCOMM - comunicações de canal nomeado
- JBBSERVICE - rastreio de serviço específico da plataforma Windows
- JBBVERBINFO - informações de verbo detalhadas
- ALL\_JBB - sinalizador de rastreio agregado que inclui todas as configurações acima

Configurações de Rastreio para o cliente de backup-archive especificado em dsm.opt:

- JOURNAL - rastreio de backup baseado em diário

## Classes de Rastreio do Cliente

O cliente fornece classes de rastreio individuais e agregadas. Classes de rastreio agregadas são um atalho para a ativação de muitas classes de rastreio relacionadas, simplesmente especificando o nome da classe de rastreio agregada. Para as classes de rastreio documentadas, pode haver referências para classes de rastreio que são ativadas como parte de uma classe de rastreio agregada, mas não explicitamente discutidas.

As classes de rastreio em Tabela 12 na página 155 são as classes de rastreio que geralmente são solicitadas ou usadas para diagnosticar problemas. A classe de rastreio deve ser usada com as opções TRACEFLAG no arquivo dsm.opt.

Tabela 12. Classes de Rastreio

Classe de Rastreio	descrição	Recomendação
ALL_BACK	Exibe informações gerais de processo de backup para o cliente. Agregado das classes de rastreio TXN, INCR, POLICY e PFM e implicitamente incluído na classe de rastreio SERVICE.	Use esta classe de rastreio para problemas relacionados a backups seletivos ou incrementais.
ALL_FILE	Exibe informações gerais de processo de backup para o cliente. Agregado de classes de rastreio DIROPS, FILEOPS e FIOATTRIBS e implicitamente incluídas na classe de rastreio SERVICE.	Use esta classe de rastreio para problemas que estão relacionados à leitura e gravação de dados e à obtenção de informações de atributos do arquivo.
ALL_IMAGE	Exibe as informações de processamento de imagem para o cliente. Agregado de várias classes de rastreio relacionadas à imagem e implicitamente incluídas na classe de rastreio SERVICE.	Use esta classe de rastreio para problemas que estão relacionados a todos os aspectos de operações de backup e restauração da imagem do volume.
ALL_JBB	Exibe informações de processo de backup baseado em diário para o cliente. Agregado de várias classes de rastreio relacionadas ao backup baseado em diário e implicitamente incluídas na classe de rastreio SERVICE.	Use esta classe de rastreio para problemas que estão relacionados a todos os aspectos de backups baseados em diário.
ALL_NAS	Exibe informações de processamento de NDMP para o cliente. Agregado de várias classes de rastreio relacionadas ao NDMP e implicitamente incluídas na classe de rastreio SERVICE.	Use esta classe de rastreio para problemas que estão relacionados a todos os aspectos de operações de backup e restauração NDMP.
ALL_SESS	Exibe todas as informações de sessão e de verbo que são enviadas entre o cliente e o servidor. Agregado de classes de rastreio SESSION, VERBINFO, SESSVERB, VERBADMIN e VERBDETAIL. Todas as classes de rastreio nesse agregado são implicitamente incluídas na classe de rastreio SERVICE, exceto VERBDETAIL.	Use esta classe de rastreio para problemas relacionados à sessão do cliente e do servidor, tais como tempos limite de comunicação, violações de protocolos e instâncias nas quais o cliente parece estar interrompido e aguardando o servidor, ou vice-versa.

Tabela 12. Classes de Rastreio (continuação)

Classe de Rastreio	descrição	Recomendação
ALL_SNAPSHOT	Exibe informações relacionadas a operações de captura instantânea do volume de volume. Agregado de várias classes de rastreio relacionadas à captura instantânea do volume e implicitamente incluídas na classe de rastreio SERVICE.	Use esta classe de rastreio para determinar problemas que estão relacionados a capturas instantâneas do volume que são usadas em operações backup de imagem on-line e de suporte a arquivos abertos.
ALL_WAS	Exibe as informações de processamento Web Application Server (WAS) para o cliente. Agregado de várias classes de rastreio relacionadas ao WAS e implicitamente incluído na classe de rastreio SERVICE.	Use esta classe de rastreio para problemas que estão relacionados a todos os aspectos de operações de backup e restauração WAS.
AUDIT	Exibe informações de auditoria para processo de backup e restauração. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para manter o registro dos arquivos processados, confirmados e restaurados em um arquivo.
CLIENTTYPE	Exibe o tipo de cliente em cada linha da saída de rastreio.	Use esta classe de rastreio para situações de rastreio em que mais de um componente do cliente está envolvido, tais como o aceitante do cliente e o agente do sistema de arquivos.
COMPRESS	Exibe informações de compactação. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para determinar a quantidade de dados compactados em uma base por arquivo.
DELTA	Exibe informações de processamento de backup de subarquivo adaptável. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para determinar erros em operações de backup de subarquivo adaptável e restauração.
DIOPS	Exibe operações de leitura e gravação de diretório. Parte dos agregados de rastreio SERVICE e ALL_FILE.	Use esta classe de rastreio quando ocorrerem problemas em um diretório de leitura ou gravação.
DOMAIN	Exibe informações de processamento de domínio incremental. Parte dos agregados de rastreio SERVICE.	Use esta classe de rastreio para determinar como instruções DOMAIN são resolvidas durante o processo de backup, tais como problemas na resolução do domínio ALL-LOCAL.

Tabela 12. Classes de Rastreio (continuação)

Classe de Rastreio	descrição	Recomendação
ENCRYPT	Exibe informações de criptografia de dados. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para determinar se um arquivo está incluído no processo de criptografia.
ERROR	Exibe informações de erro específicas do sistema operacional. Parte do agregado de rastreio SERVICE.	Use essa classe de rastreio para determinar os códigos de erro que são gerados pelo sistema operacional.
FILEOPS	Exibe operações de leitura e gravação de arquivo. Parte dos agregados de rastreio SERVICE e ALL_FILE.	Use esta classe de rastreio quando ocorrerem problemas em uma operação de abertura, leitura, gravação ou fechamento de arquivo.
FIOATTRIBS	Exibe comparações dos atributos de arquivos entre a versão do cliente local e a versão ativa no servidor. Parte dos agregados de rastreio SERVICE, ALL_BACK e ALL_FILE.	Use esta classe de rastreio para determinar por que foi feito backup de um arquivo durante um backup incremental.
INCR	Exibe comparações de processamento da lista incremental entre o cliente e o servidor. Parte dos agregados de rastreio SERVICE e ALL_BACK.	Use essa classe de rastreio para determinar se os arquivos são candidatos para backup incremental, especialmente com a classe de rastreio FIOATTRIBS.
INCLEXCL	Exibe o status de inclusão-exclusão para o objeto que está sendo processado. Este sinalizador também é usado para a função Visualização.	Use esta classe de rastreio para determinar qual objeto (geralmente arquivo ou diretório) foi incluído ou excluído durante o backup-archive/visualização.
MEMORY	Exibe pedidos de alocação e liberação de memória. Esta classe de rastreio grava uma grande quantidade de informações no arquivo de rastreio e não está incluída em nenhuma das classes agregadas.	Use esta classe de rastreio para determinar fugas de memória, picos de memória e outros problemas relacionados à memória.
OPTIONS	Exibe opções de processamento atuais. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para determinar quais opções estão em vigor para a sessão atual e para problemas ao aceitar as opções de processamento dos conjuntos de opções do cliente de servidor.

Tabela 12. Classes de Rastreio (continuação)

Classe de Rastreio	descrição	Recomendação
PASSWORD	Exibe informações de arquivo ao arquivo de senhas (não mostra senhas). Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para determinar problemas com a leitura das senhas do servidor do armazenamento local, por exemplo, erros PASSWORDACCESS=GENERATE.
PID	Exibe o ID do processo em cada instrução de rastreio. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para diagnosticar problemas que podem envolver vários processos.
POLICY	Exibe informações de política disponíveis para o cliente de backup-archive. Parte dos agregados de rastreio SERVICE e ALL_BACK.	Use esta classe de rastreio para ver quais políticas estão disponíveis durante uma operação de backup ou archive.
SCHEDULER	Exibe informações gerais de processamento para o planejador. Um agregado que inclui a maioria das classes de rastreio do cliente listadas nesta tabela. Agregado de todas as classes de rastreio, exceto as classes MEMORY, THREAD_STATUS e *DETAIL.	Útil em muitos casos. Essa classe de rastreio é usada para diagnosticar problemas do planejador quando a natureza do problema é desconhecida. Se o sinalizador de rastreio SCHEDULER for usado, geralmente não será necessário especificar nenhum dos outros sinalizadores de rastreio, porque ele já inclui a maioria das classes de rastreio básicas.
SERVICE	Exibe informações gerais de processamento para o cliente. Um agregado que inclui a maioria das classes de rastreio do cliente listadas nesta tabela. Agregado de todas as classes de rastreio, exceto as classes MEMORY e *DETAIL. O sinalizador de rastreio SERVICE pode gerar uma quantidade substancial de informações. Considere usar a opção TRACEMAX juntamente com o sinalizador de rastreio SERVICE.	Útil em muitos casos. Essa classe de rastreio é usada quando a natureza do problema é desconhecida. Se o sinalizador de rastreio SERVICE for usado, não será necessário especificar nenhum dos outros sinalizadores de rastreio, porque ele já inclui a maioria das classes de rastreio básicas.



Tabela 12. Classes de Rastreio (continuação)

Classe de Rastreio	descrição	Recomendação
SESSION	Exibe o mínimo de informações da sessão entre o cliente e o servidor. Parte dos agregados de rastreio SERVICE e ALL_SESS.	Use esta classe de rastreio para fornecer contexto de sessão para erros gerais de processamento ou com uma das classes de rastreio VERB*, para determinar problemas de sessão, tais como tempos limite de sessão e violações de protocolos.
SESSVERB	Exibe informações adicionais da sessão entre o cliente e o servidor. Parte dos agregados de rastreio SERVICE e ALL_SESS.	Use esta classe de rastreio para fornecer contexto de sessão para erros gerais de processamento ou com uma das classes de rastreio VERB*, para determinar problemas de sessão, tais como tempos limite de sessão e violações de protocolos.
STATS	Exibe estatísticas finais de processamento no arquivo de rastreio. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio para coletar estatísticas finais de processamento em um arquivo.
THREAD_STATUS	Exibe status do encadeamento. Parte do agregado de rastreio SERVICE.	Use esta classe de rastreio ao diagnosticar problemas relacionados ao encadeamento.
TXN	Exibe informações de processamento de transações. Parte dos agregados de rastreio SERVICE e ALL_BACK.	Use esta classe de rastreio ao diagnosticar problemas relacionados ao processamento de transação no servidor e, para esses problemas, como a transação para e é novamente tentada.
VERBDETAIL	Exibe informações detalhadas do verbo relacionadas a sessões do cliente/servidor. Parte dos agregados de rastreio ALL_SESS.	Use esta classe de rastreio para determinar o conteúdo dos verbos enviados entre o cliente e o servidor.
VERBINFO	Exibe informações do verbo relacionadas a sessões do cliente/servidor. Parte dos agregados de rastreio SERVICE e ALL_SESS.	Use esta classe de rastreio com o sinalizador de rastreio SESSION para fornecer contexto de sessão para erros gerais de processamento ou para determinar problemas de sessão, como tempos limite de sessão e violações de protocolos.

Tabela 12. Classes de Rastreio (continuação)

Classe de Rastreio	descrição	Recomendação
WIN2K	Exibe o objeto do sistema Windows ou o processamento de estado do sistema. Parte dos agregados de rastreio SERVICE. Válida apenas no cliente de backup-archive do Windows.	Use esta classe de rastreio para determinar erros com o backup ou restauração de informações de estado do sistema.

## Ativando o Rastreio do Cliente de Backup-archive

Existem dois métodos de rastreio que estão disponíveis para o cliente de backup-archive.

O primeiro método é configurar parâmetros de rastreio antes de iniciar o cliente de backup-archive. O segundo método é ativar o rastreio enquanto o cliente está executando. Escolha o método de rastreio a ser ativado.

### Ativando um Rastreio do Cliente Usando a Linha de Comandos

É possível rastrear o cliente de backup-archive disponível ativando o rastreio do cliente na linha de comandos.

#### Sobre Esta Tarefa

Conclua as etapas a seguir para ativar o rastreio do cliente na linha de comandos:

#### Procedimento

1. Determine as classes de rastreio a serem ativadas.
2. Escolha quais classes de rastreio ativar incluindo o seguinte texto no arquivo de opções do cliente dsm.opt: `traceflags <trace class name>`
3. Use um sinal de menos (-) na frente de uma classe de rastreio para desligar o rastreio para uma classe de rastreio. Certifique-se de que as classes de rastreio que possuem o rastreio desligado sejam colocados no fim da lista da classe de rastreio. Por exemplo, se desejar coletar um rastreio de SERVICE sem as classes SESSION ou SESSVERB, especifique o seguinte texto:

Correto: `traceflags service,-session,-sessverb`

Incorreto: `traceflags -session,-sessverb,service`

**Atenção:** `<nome da classe de rastreio>` pode ser uma lista de classes de rastreio delimitada por vírgulas. Por exemplo, este texto pode ser inserido como `traceflags service,verbdetail`

4. Escolha o local da saída de mensagens de rastreio, incluindo o seguinte texto no arquivo de opções do cliente: `tracefile <nome do arquivo>`.

O nome *tracefile* deve ser completo, por exemplo:

**Windows** `tracefile c:\service\trace.out`

**AIX** **Linux** `tracefile /home/spike/trace.out`

**Mac OS X** `tracefile trace.txt`

5. Configure o tamanho máximo do arquivo de rastreio 1 - 4.294.967.295 MB, especificando a seguinte variável no arquivo de opções do cliente: `tracemax <size in mb>`

Se for especificado um valor máximo, o cliente começará a gravar informações a partir do início do arquivo de rastreo (ou seja, quebra) quando o rastreo atingir seu tamanho máximo. Estas informações podem ser úteis se você estiver tentando capturar um evento que ocorre no final de um processo de execução longa. Por exemplo, para especificar um tamanho máximo de arquivo de rastreo de 10 MB: `tracemax 10` Depois que o arquivo de rastreo atingir o limite que foi especificado com `tracemax`, “Continuação no início do arquivo” será gravado no final do arquivo de rastreo e o rastreo continuará a partir do início do arquivo. O final do arquivo de rastreo é indicado com “END OF DATA.” É possível localizar o final do rastreo procurando esta cadeia. Se for especificado um tamanho de `TRACEMAX` de 1001 ou maior e `TRACESEGSIZE` não for especificado, o arquivo de rastreo será automaticamente dividido em vários segmentos de 1000 MB por segmento (consulte a discussão de `TRACESEGSIZE`).

É possível optar por permitir que o cliente divida o rastreo em segmentos menores (1 a 1.000 MB por segmento), especificando a seguinte variável no arquivo de opções do cliente: `traceseysize <trace segment size in MB>`

Quando o rastreo for dividido em pequenos segmentos, você poderá gerenciar facilmente grandes quantidades de dados de rastreo, evitando os problemas associados à compactação de grandes arquivos e eliminando a tarefa de usar um utilitário “file splitter” separado. Por exemplo, emita o seguinte comando para especificar um tamanho de segmento de rastreo de 200 MB: `traceseize 200`

Um nome de segmento do arquivo de rastreo é especificado com a opção `tracefile`, mais uma extensão que indica o número do segmento. Por exemplo, se você especificar `tracefile tsmtrace.out` e `traceseize 200`, o rastreo será segmentado em vários arquivos separados que não ultrapasse 200 MB cada um com nomes de arquivo `tsmtrace.out.1`, `tsmtrace.out.2` e assim por diante. Ao especificar o tamanho do segmento, não use nenhum dos separadores de vírgula:

Correto: `tracemax 1000`

Incorreto: `tracemax 1,000`

Se você usar a opção `TRACESEGSIZE`, os segmentos do arquivo de rastreo serão nomeados usando o nome especificado no arquivo de opções com uma extensão extra usando o número de segmentos. Por exemplo, `trace.out.1`

6. Execute a operação que exhibe o problema.

## O que Fazer Depois

O rastreo também pode ser configurado e iniciado chamando o cliente a partir de um prompt de comandos e especificando os sinalizadores definidos anteriormente. Por exemplo:

```
dsmc -traceflags=service,verbdetail -tracefile=tsmtrace.out  
-tracemax=2500 -traceseize=200
```

### Referências relacionadas:

“Classes de Rastreo do Cliente” na página 154

## Ativando um Rastreo Enquanto o Cliente Está em Execução

É possível rastrear o cliente de backup-archive disponível enquanto o cliente está em execução.

### Antes de Iniciar

- O cliente de backup-archive deve ser instalado para usar o rastreo dinâmico.
- A opção DSMTRACELISTEN YES deve entrar em vigor quando o cliente for iniciado.
  - **AIX** **Linux** Essa opção é especificada no arquivo de opções do sistema (dsm.sys) na sub-rotina que o cliente usa. Os usuários devem estar com login efetuado como root para usarem dsmtrace.
  - **Windows** Essa opção é especificada no arquivo de opções do sistema (geralmente dsm.opt). Os usuários devem estar com login efetuado como membro do grupo Administradores.

Quando o cliente é iniciado, ele inicia um encadeamento de “listener de rastreo” separado. Este encadeamento “atende” em um canal nomeado, aguardando ser contactado pelo utilitário dsmtrace. Para tornar o nome do canal nomeado exclusivo, o ID do processo do cliente (PID) faz parte do nome do canal. Quando você usa dsmtrace para configurar o rastreo, ele contata o cliente por meio do canal nomeado no qual o cliente está atendendo e o transmite para a operação de configuração de rastreo preferencial. O cliente transmite então os resultados da operação de volta a dsmtrace por meio de outro canal de saída nomeado de forma semelhante. dsmtrace exibe os resultados no console. O cliente iniciará o encadeamento do listener de rastreo apenas quando a opção do cliente DSMTRACELISTEN YES estiver em vigor. Se DSMTRACELISTEN NO estiver em vigor, o encadeamento do listener não será iniciado e o rastreo dinâmico não estará disponível para esse cliente. DSMTRACELISTEN NO é o valor padrão.

### Sobre Esta Tarefa

As etapas para reunir um rastreo do cliente são as seguintes:

#### Procedimento

1. Pare o cliente de backup-archive.
2. Configure o arquivo de opções do cliente com as opções de rastreo preferenciais.
3. Reinicie o cliente de backup-archive e reproduza o problema.
4. Pare o cliente de backup-archive.
5. Remova as opções de rastreo do arquivo de opções do cliente de backup-archive.
6. Envie o arquivo de rastreo resultante para o suporte técnico IBM para análise.

Também é possível usar o utilitário dsmtrace para iniciar, parar e configurar o rastreo do cliente dinamicamente, sem precisar parar o cliente ou modificar o arquivo de opções. O rastreo dinâmico é útil principalmente quando for necessário rastrear somente o início de uma operação do cliente de backup-archive de longa execução, ou quando for necessário iniciar o rastreo após o cliente de backup-archive estar em execução por algum tempo.

O utilitário dsmtrace inclui os seguintes recursos:

- Identifique os processos em execução e seus PIDs de processo
- Ativar o rastreo do cliente
- Desativar o rastreo do cliente

- Consultar o status de rastreo do cliente

A tabela a seguir resume a disponibilidade deste recurso:

*Tabela 13. Disponibilidade do Utilitário dsmtrace*

Componente do Cliente	Nome do Programa do AIX ou Linux	Nome do Programa do Windows
Cliente de Backup-Archive (linha de comandos)	dsmc	dsmc.exe
Cliente de Backup-Archive (GUI)	N/A	dsmagent.exe
Aceitante do cliente	dsmcad	dsmcad.exe
Agente de Cliente Remoto	dsmagent	dsmagent.exe
Serviço do Planejador	N/A	dsmcsvc.exe
Serviço de Diário	N/A	tsmjbbd.exe
Data Protection para Domino (linha de comandos)	domdsmc	domdsmc.exe
Data Protection para Domino (GUI)	N/A	domdsm.exe
Data Protection para Microsoft Exchange (linha de comandos)	N/A	tdpexcc.exe
Data Protection para Microsoft Exchange (GUI)	N/A	tdpexc.exe
Data Protection para Microsoft SQL Server (linha de comandos)	N/A	tdpsqlc.exe
Data Protection para Microsoft SQL Server (GUI)	N/A	tdpsql.exe

**Nota:**

- A coluna central na Tabela 13 inclui o Macintosh OS X.
- O rastreo para os componentes do Data Protection destina-se apenas à interface de programação de aplicativo (API) do IBM Spectrum Protect.
- O rastreo da API do IBM Spectrum Protect está disponível com qualquer aplicativo multiencadeado que usa a API do IBM Spectrum Protect. O nome do arquivo executável é o nome do programa aplicativo que carrega a API.

**Exemplo**

O exemplo a seguir mostra como ativar o rastreo do cliente durante a execução do cliente:

1. Identifique o PID do processo do cliente de backup-archive que você deseja rastrear (certifique-se de que DSMTRACELISTEN YES esteja em vigor). Emita o seguinte comando para mostrar todas as instâncias em execução do cliente:  
dsmtrace query pids

Saída de exemplo:

```
D:\tsm>dsmtrace query pids
```

```
IBM Spectrum Protect
dsmtrace utility
dsmtrace Version 5, Release 3, Level 0.0
```

```
dsmtrace date/time: 10/24/2004 21:07:36
(c) Copyright by IBM Corporation and other(s) 1990, 2004. Todos
os Direitos Reservados.
```

PROCESS ID	PROCESS OWNER	DESCRIPTION	EXECUTABLE NAME
4020	andy	Backup-Archive Client (CLI)	dsmc.exe

```
D:\tsm>
```

**Importante:** Linux O modelo de encadeamento para algumas versões do Linux é executar cada encadeamento como um processo separado, o que significa que, ao consultar informações do processo, é possível ver vários processos para cada instância do cliente. O processo que deve ser identificado é o processo pai dsmc. Por exemplo:

```
fvtnlinuxppc:/opt/tivoli/tsm/client/ba/bin # dsmtrace q p
```

```
IBM Spectrum Protect
dsmtrace utility
dsmtrace Version 5, Release 3, Level 0.0
dsmtrace date/time: 10/24/04 08:07:37
(c) Copyright by IBM Corporation and other(s) 1990, 2004. Todos
os Direitos Reservados.
```

PROCESS ID	PROCESS OWNER	DESCRIPTION	EXECUTABLE NAME
28970	root	Backup-Archive Client (CLI)	dsmc
28969	root	Backup-Archive Client (CLI)	dsmc
28968	root	Backup-Archive Client (CLI)	dsmc
28967	root	Backup-Archive Client (CLI)	dsmc

```
fvtnlinuxppc:/opt/tivoli/tsm/client/ba/bin #
```

Nessa situação, emita o comando **PS** para identificar o processo pai dsmc:

```
linuxppc:~ # ps -ef | grep dsmc
```

root	28967	1151	0	Oct22 pts/16	00:00:00	dsmc
root	28968	28967	0	Oct22 pts/16	00:00:00	dsmc
root	28969	28968	0	Oct22 pts/16	00:00:00	dsmc
root	28970	28968	0	Oct22 pts/16	00:00:00	dsmc
root	24092	24076	0	08:15 pts/93	00:00:00	grep dsmc

```
linuxppc:~ #
```

Observe que o pai para processos 28969 e 28970 é 28968. O pai para 28968 é 28967. O pai para 28967 é 1151, mas o processo 1151 não aparece nesta saída de exibição. O processo 1151 é o processo que iniciou o dsmc. Portanto, o ID do processo pai correto é 28967.

2. Emita o seguinte comando para ativar o rastreamento no cliente:

```
dsmtrace enable 4020 -traceflags=service -tracefile=d:\trace.txt
```

Saída de exemplo:

```
C:\arquivos de programas\tivoli\tsm\baclient>dsmtrace enable 4020
-traceflags=service -tracefile=d:\trace.txt
```

```
IBM Spectrum Protect
dsmtrace utility
dsmtrace Version 5, Release 3, Level 0.0
dsmtrace date/time: 10/24/2004 21:45:54
(c) Copyright by IBM Corporation and other(s) 1990, 2004. Todos
os Direitos Reservados.
```

```
ANS2805I Tracing has been enabled.
```

```
C:\arquivos de programas\tivoli\tsm\baclient>
C:\arquivos de programas\tivoli\tsm\baclient>
```

**Importante:** Quando estiver rastreando um aplicativo da API, a opção `-pipenameprefix` deverá ser incluída.

- **AIX** **Linux** Use o prefixo `/tmp/TsmTraceTargetAPI`
- **Windows** Use o prefixo `\\.\pipe\TsmTraceTargetAPI`

3. Quando forem coletados dados de rastreamento suficientes, desative o rastreamento emitindo o seguinte comando:

```
dsmtrace disable 4020
```

Saída de exemplo:

```
C:\arquivos de programas\tivoli\tsm\baclient>dsmtrace disable 4020
```

```
IBM Spectrum Protect
dsmtrace utility
  dsmtrace Version 5, Release 3, Level 0.0
  dsmtrace date/time: 10/24/2004 21:47:43
  (c) Copyright by IBM Corporation and other(s) 1990, 2004. Todos
  os Direitos Reservados.
```

```
ANS2802I Tracing has been disabled.
```

Outros exemplos de ativação do rastreamento do cliente durante a execução do cliente são definidos na lista a seguir:

**dsmtrace query pids**

Este comando exibe todos os processos em execução cujos nomes são listados na tabela na seção Segundo Plano.

**dsmtrace query pids -filter=\***

Este comando exibe todos os processos em execução.

**dsmtrace query pids -filter=dsm\***

Este comando exibe todos os processos em execução cujos nomes começam com "dsm"

**dsmtrace query pids -filter=dsm?**

Este comando exibe todos os processos em execução cujo nome começa com "dsm" mais um outro caractere.

**dsmtrace enable 2132 -traceflags=service -tracefile=c:\trace.txt**

Este comando ativa o rastreamento de SERVICE para o processo 2132. A saída de rastreamento é gravada no arquivo `c:\trace.txt`.

**dsmtrace enable 2132 -traceflags=-extrc**

Este comando desativa o rastreamento de extrc para o processo 2132 (provavelmente o rastreamento já está em execução para este processo).

**dsmtrace enable 4978 -traceflags=fileops -tracefile=/tmp/dsmtrace.out -tracemax=1000 -tracesegsize=200**

Este comando ativa o rastreamento de FILEOPS para o processo 4978. O rastreamento é gravado nos arquivos `/tmp/dsmtrace.out.1`, `/tmp/dsmtrace.out.2` e assim por diante, com cada arquivo tendo mais de 200 MB. Quando forem gravados 1000 MB, o rastreamento será quebrado de volta para `/tmp/dsmtrace.out.1`.

**dsmtrace query trace 4978 -on**

Este comando exibe as informações de rastreamento básicas e lista os sinalizadores de rastreamento que estão ativados para o processo 4978.

### **dsmttrace disable 4978**

Este comando desativa o rastreo para o processo 4978.

### **dsmttrace disable 364 -pipenameprefix=/tmp/TsmTraceTargetAPI**

Este comando desativa o rastreo para o processo aplicativo da API 364.

## **Problemas e Limitações de Rastreo Conhecidos**

Os problemas e limitações conhecidos dos processos de rastreo são reunidos para ajudá-lo a resolver problemas que podem ser encontrados durante a execução de um processo de rastreo.

- Se o rastreo não estiver atualmente ativo para um processo e dsmttrace for usado apenas com a opção -TRACEFLAGS, por exemplo, **dsmttrace enable 2346 -traceflags=service**, você ainda verá a seguinte mensagem:


ANS2805I Tracing has been enabled.

Neste caso, os sinalizadores de rastreo foram ativados, mas o rastreo não estará ativo até que seja especificado um arquivo de rastreo usando a opção -TRACEFILE.

- Não use o comando dsmttrace enable para iniciar o rastreo da interface de programação de aplicativo (API) para aplicativos Data Protection se o aplicativo Data Protection for executado de uma maneira que não o faz conectar-se ao servidor IBM Spectrum Protect. Por exemplo, a interface da linha de comandos do Data Protection para IBM Domino possui vários desses comandos:

- domdsmc help
- domdsmc set
- domdsmc query domino
- domdsmc query pendingdbs
- domdsmc query preferences

Se você usar dsmttrace para ativar o rastreo para esses comandos, o resultado poderá ser uma parada do processo dsmttrace e (somente AIX e Linux) um canal nomeado residual no diretório /tmp.

-  **Windows** Você deve ter efetuado login com uma conta administrativa local para usar dsmttrace.
- Você deve ter efetuado login como root para usar dsmttrace. Se um processo do cliente parar ou for interrompido, ele poderá deixar um canal nomeado (FIFO UNIX) no diretório /tmp. Estes FIFOs possuem nomes que começam com TsmTrace e incluem um número de ID do processo (PID). Se um processo do cliente parar ou for interrompido e, em seguida, for iniciado um novo processo do cliente cujo PID corresponde ao do FIFO residual antigo, o encadeamento do listener de rastreo poderá não iniciar. Os FIFOs antigos com números de processo que não correspondem aos FIFOs dos processos do IBM Spectrum Protect em execução podem ser excluídos com segurança. NÃO exclua o FIFO de um processo em execução.
- O modelo de encadeamento para algumas versões do Linux é executar cada encadeamento como um processo separado, o que significa que, quando você consultar as informações de processo, poderá ver vários processos para cada instância do cliente. O processo que você precisa identificar é o processo pai dsmt.
- Quando várias instâncias do mesmo programa estão executando, você deve identificar o PID da instância que deseja rastrear. Nessa situação, informações como informações do processo do sistema operacional podem estar disponíveis para ajudá-lo a identificar o PID necessário. Por exemplo, se desejar rastrear o dsmt que está sendo executado pelo usuário 'andy' e houver duas instâncias do



dsmc, uma pertencente ao usuário 'andy' e a outra pertencente ao usuário 'kevin', será possível usar o proprietário do processo para identificar qual processo rastrear.

- Se um arquivo de opções contiver uma opção falsa e o cliente não for iniciado, será possível ver alguns erros de canal nomeado no arquivo `dsmerror.log`. Essas mensagens de erro podem ser ignoradas com segurança.

## Opções de Rastreio

O rastreio possui várias opções que podem ser empregadas.

### DSMTRACEListen

#### DSMTRACEListen No | Yes

- |            |  |
|------------|--|
| <b>Não</b> | O cliente não inicia o encadeamento do listener de rastreio e o rastreio dinâmico não está disponível. O padrão é Não. |
| <b>Sim</b> | O cliente inicia o encadeamento do listener de rastreio e o rastreio dinâmico está disponível.                         |

**Windows** A opção `DSMTRACEListen` é especificada no arquivo de opções do cliente (normalmente, `dsm.opt`).

### dsmtrace

#### dsmtrace enable <pid> <options>

Use este comando para iniciar ou modificar o rastreio para um processo.

**pid** O ID do processo (PID) para o cliente. Use `dsmtrace query pids` ou os recursos de seu sistema operacional para identificar o PID correto.

**options**  
As opções de rastreio do cliente.

#### dsmtrace disable <pid>[<options>]

Use este comando para parar o rastreio para um processo. O arquivo de rastreio é fechado e os sinalizadores de rastreio, tamanho máximo de rastreio, tamanho máximo de segmento de rastreio e nome de arquivo de rastreio são todos limpos.

**<pid>** O PID do cliente. Use `dsmtrace query pids` ou os recursos de seu sistema operacional para identificar o PID correto.

**<options>**  
As opções de rastreio do cliente.

#### dsmtrace help

Este comando exibe a sintaxe básica para `dsmtrace`.

#### dsmtrace query pids [-Filter=<spec>]

**<spec>**

A especificação de filtro de nome do processo do cliente, que pode incluir os caracteres curingas "?" (corresponde exatamente a um caractere) ou "\*" (corresponde a zero ou mais caracteres).

Se nenhum filtro for especificado, o comportamento padrão será exibir informações do processo para quaisquer instâncias em execução dos nomes de programas listados na tabela na seção Segundo Plano, acima.

**Importante:** AIX Linux Ao usar FILTER, coloque o símbolo \* antes e após o texto de procura. Este ajuste é necessário porque o nome do arquivo executável geralmente inclui o caminho na frente dele e, em alguns casos, o nome do arquivo executável pode ter caracteres adicionais no final dele. Por exemplo:

- /opt/tivoli/tsm/client/ba/bin/dsmc
- domdsmc\_DominoUserID

Portanto, em vez de -filter=dsmc ou -filter=domdsmc, use -filter=\*dsmc\* ou -filter=\*domdsmc\*.

**dsmtrace query trace <pid> [<options>] [<displayType>] [-All | -ON | -Off | -BASic]**

**<pid>** O ID do processo (PID) para o cliente. Use dsmtrace query pids ou os recursos de seu sistema operacional para identificar o PID correto.

**<options>**  
As opções de rastreamento do cliente.

**<displayType>**  
O tipo de exibição pode ser uma das seguintes entradas:

- All** Exibe todos os sinalizadores de rastreamento e, para cada sinalizador, indica se ele está ativado ou desativado. As informações mostradas com o tipo de exibição -BASic também são incluídas.
- ON** Exibe os nomes dos sinalizadores de rastreamento que estão ativados. As informações mostradas com o tipo de exibição -BASic também são incluídas.
- Off** Exibe os nomes dos sinalizadores de rastreamento que estão desativados. As informações mostradas com o tipo de exibição -BASic também são incluídas.
- BASic** Exibe o nome do arquivo de rastreamento e os tamanhos máximo de rastreamento e do segmento de rastreamento. Este tipo de exibição também indica se o rastreamento está ativado ou desativado.

## **-PIPENameprefix**

**-PIPENameprefix=<pipeNamePrefix>**

A opção -PIPENameprefix deve ser usada durante o rastreamento de aplicativos da interface de programação de aplicativo (API):

- AIX Linux Use o prefixo /tmp/TsmTraceTargetAPI
- Windows Use o prefixo \\.\pipe\TsmTraceTargetAPI

## **-TRACEFile**

**-TRACEFile=<traceFileName>**

A opção -TRACEFile deve especificar um nome do arquivo válido no qual o rastreamento é gravado. Se o rastreamento já estiver em execução, esta opção não terá nenhum efeito.

## -TRACEFLags

### -TRACEFLags=<*traceFlags*>

Especifique um ou mais sinalizadores de rastreo. Geralmente, o sinalizador de rastreo SERVICE é usado. Separe vários sinalizadores de rastreo com uma vírgula. Os sinalizadores de rastreo também podem ser desativados prefixando o nome do sinalizador com um sinal de menos. Ao combinar sinalizadores de rastreo que você deseja ativar com sinalizadores de rastreo que deseja desativar, coloque os sinalizadores que serão desativados no final da lista. Por exemplo, se deseja ativar o rastreo SERVICE, exceto para VERBDETAIL, especifique -TRACEFLAGS=SERVICE,-VERBDETAIL. Se o rastreo já estiver em execução, esta opção poderá ser usada para ativar sinalizadores de rastreo adicionais ou desativar sinalizadores de rastreo.

## -TRACEMax

### -TRACEMax=<*maximumTraceSize*>

Esta opção limita o comprimento máximo do arquivo de rastreo para o valor especificado (por padrão, o arquivo de rastreo aumenta indefinidamente). Quando o comprimento máximo é atingido, o rastreo volta novamente para o início do arquivo. Especifique um valor em MB entre 1 e 4095. Se o rastreo já estiver executando, essa opção não terá efeito.

## -TRACESegsize

### -TRACESegsize=<*maximumTraceSegmentSize*>

Esta opção é usada quando você prevê um grande arquivo de rastreo e deseja que ele seja gravado em segmentos menores, mais facilmente gerenciados. Cada segmento não é maior que o tamanho especificado. Quando essa opção é usada, um número de segmento é anexado ao nome do arquivo de rastreo de cada segmento. Especifique um valor em MB entre 1 e 1000. Se o rastreo já estiver executando, essa opção não terá efeito.

#### Nota:

- Para ativar o rastreo para um processo é necessário usar as opções -TRACEFLAGS e -TRACEFILE (e -PIPEPREFIX ao rastrear um aplicativo da API).
- Para modificar sinalizadores de rastreo para um processo existente, use -TRACEFLAGS (e -PIPEPREFIX ao rastrear um aplicativo da API).
- Se precisar modificar o nome do arquivo de rastreo, o tamanho máximo de rastreo ou o tamanho máximo do segmento de rastreo, primeiro é necessário desativar todo o rastreo (consulte o comando **dsmttrace disable**).

## Determinando se os dados são criptografados ou compactados durante o archive de backup usando rastreo

É necessário executar várias etapas para determinar se os dados durante o backup-archive são compactados ou criptografados, ou ambos.

### Procedimento

1. Inclua as opções de rastreo que são listadas no arquivo de opções do cliente antes de fazer backup ou de arquivar objetos:
  - TRACEFILE <nome do arquivo de rastreo>
  - TRACEFLAGS api api\_detail
2. Examine o arquivo de rastreo após a operação e localize uma instrução que seja semelhante à seguinte:

```
dsmSendObj ENTRY:... objNameP: <the file name>
```

Esta saída é seguida pela mensagem de rastreo a seguir, que indica se o objeto foi compactado, criptografado, ou compactado e criptografado:

```
tsmEndSendObjEx: Total de bytes enviados * *, encryptType é *** encryptAlg é ***  
compress é *, totalCompress é * * totalLFBytesSent * *
```

```
+-----+  
| encryptType/compress | 0 | 1 |  
+-----+  
| NO | não compactado, não criptografado | compactado, não criptografado |  
| CLIENTENCRKEY | não compactado, criptografado | compactado, criptografado |  
| USER | não compactado, criptografado | compactado, criptografado |  
+-----+
```

Como alternativa, seu próprio aplicativo pode determinar o tipo/intensidade de criptografia e compactação de seus dados usando a chamada de função **dsmEndSendObjEx** e a estrutura de dados **dsmEndSendObjExOut\_t**.

```
/*-----+  
| Definição de tipo para dsmEndSendObjExOut_t  
+-----*/  
typedef struct dsmEndSendObjExOut_t  
{  
    dsUInt16_t      stVersion;          /* versão da estrutura */  
    dsStruct64_t    totalBytesSent;      /* total de bytes lidos do apl. */  
    dsmBool_t       objCompressed;       /* foi compactado por objeto */  
    dsStruct64_t    totalCompressSize;   /* tamanho total após compactação */  
    dsStruct64_t    totalLFBytesSent;    /* total de bytes enviados sem a LAN */  
    dsUInt8_t       encryptionType;     /* tipo de criptografia utilizado */  
}dsmEndSendObjExOut_t;
```

objCompressed - Um sinalizador que exibe se o objeto tiver sido compactado.  
encryptionType - Um sinalizador que exibe o tipo de criptografia.

Por exemplo:

```
...  
rc = dsmEndSendObjEx(&endSendObjExIn, &endSendObjExOut);  
if (rc)  
{  
    printf("*** dsmEndSendObjEx failed: ");  
    rcApiOut(dsmHandle, rc);  
}  
else  
{  
    printf("Compression:      %s\n",  
endSendObjExOut.objCompressed == bTrue ? "YES" : "NO");  
  
    printf("Encryption:        %s\n",  
endSendObjExOut.encryptionType & DSM_ENCRYPT_CLIENTENCRKEY ?
```

```

"CLIENTENCRKEY" :
endSendObjExOut.encryptionType & DSM_ENCRYPT_USER ? "USER" : "NO");
printf("Encryption Strength: %s\n\n",
endSendObjExOut.encryptionType & DSM_ENCRYPT_AES_256BIT ? "AES_256BIT" :
endSendObjExOut.encryptionType & DSM_ENCRYPT_AES_128BIT ? "AES_128BIT" :
endSendObjExOut.encryptionType & DSM_ENCRYPT_DES_56BIT ? "DES_56BIT" :
"NONE");
}
...

```

## O que Fazer Depois

Para obter mais informações, consulte *Chamadas de Função da API em Usando a Interface de Programação de Aplicativos*.

---

## Dados de Rastreo para a API

É possível ativar o rastreo para a Interface de Programação de Aplicativos (API).

Para ativar o rastreo para a API do IBM Spectrum Protect, inclua as seguintes linhas no arquivo `dsm.opt` ou outro arquivo designado como o arquivo de opções do cliente:

```

TRACEFILE trace file name
TRACEFLAGS trace flags

```

### *trace file name*

O nome do arquivo no qual você deseja gravar os dados de rastreo.

### *trace flags*

A lista de sinalizadores de rastreo a serem ativados. Separe cada sinalizador de rastreo com um espaço. Os seguintes sinalizadores de rastreo são específicos da API do IBM Spectrum Protect:

**api**      Informações sobre as chamadas de função da API

#### **api\_detail**

Informações detalhadas sobre as chamadas de função da API

Você também pode especificar outro cliente de backup-archive e sinalizações de rastreo da API do IBM Spectrum Protect. Consulte a documentação do cliente de backup-archive para obter uma lista das classes de rastreo disponíveis. Por exemplo:

- TRACEFILE /log/trace.out
- TRACEFLAGS api api\_detail verbinfo verbdetail time stamp

**Importante:** Se você não tiver permissão de gravação para o arquivo apontado pela opção TRACEFILE, `dsmSetup` ou `dsmInitEx/dsmInit` falhará com o código de retorno DSM\_RC\_CANNOT\_OPEN\_TRACEFILE (426).

Para ativar o rastreo para API multiencadeada após o início de um aplicativo, use o utilitário `dsmtrace`. O utilitário `dsmtrace` permite que você ative o rastreo enquanto o problema está ocorrendo, sem precisar ativá-lo constantemente. Consulte a seção *dsmtrace*.

---

## Rastreando o Agente do Tivoli Monitoring for Tivoli Storage Manager em um Sistema AIX ou Linux

AIX

Linux

Usando o Tivoli Monitoring for Tivoli Storage Manager, você pode criar e configurar instâncias do agente que monitoram servidores IBM Spectrum Protect. Pare todas as instâncias do agente, modifique os arquivos de configuração e reinicie as instâncias do agente para ativar o rastreo dos agentes de monitoramento para servidores no AIX ou Linux.

### Sobre Esta Tarefa

Antes de ativar o rastreo, também é possível abrir a área de trabalho Log de Agente do Tivoli Enterprise Portal e visualizar as atividades do agente. A área de trabalho Log de Agente contém informações sobre qualquer servidor IBM Spectrum Protect que tenha uma instância do agente que esteja configurada para monitorá-lo. É possível ver a saída do arquivo de rastreo sem precisar ativar o arquivo de rastreo, usando o grupo de atributos Log de Agente.

Conclua as seguintes etapas para ativar o rastreo:

### Procedimento

1. Em uma linha de comandos, acesse o seguinte diretório:

```
cd install_dir/itm/bin
```

em que *install\_dir* é o diretório de instalação do agente de monitoramento. O diretório de instalação padrão é `/opt/tivoli/tsm/reporting`. Se você instalou o agente de monitoramento em um servidor IBM Tivoli Monitoring existente, acesse o diretório `bin`. O diretório de instalação padrão é `/opt/IBM/ITM`.

2. Pare as instâncias do agente de monitoramento concluindo uma das seguintes etapas:
  - Pare os agentes de monitoramento na interface gráfica com o usuário do CandleManage, emitindo os seguintes comandos:
    - a. Execute o programa CandleManage emitindo os seguintes comandos:

```
./CandleManage &
```
    - b. Na janela Manage Tivoli Enterprise Monitoring Services, verifique se o agente de monitoramento está interrompido. Se ele não tiver sido interrompido, selecione a instância do agente aplicável, clique com o botão direito do mouse e selecione **Parar**.
  - Pare os agentes de monitoramento a partir da linha de comandos, emitindo os seguintes comandos:
    - a. 

```
./itmcmd agent -o instance_name stop sk
```
3. Para garantir que todos os agentes tenham sido interrompidos, conclua as seguintes etapas:
  - a. Aguarde até que a interface gráfica de CandleManage informe que o agente foi interrompido.
  - b. Verifique se o seguinte processo está executando emitindo o seguinte comando:

```
ps -ef | grep -i SK
```
  - c. Se o processo estiver executando, pare-o emitindo o seguinte comando:

```
kill -9 process_ID
```

4. Localize o diretório no qual os arquivos de configuração estão armazenados emitindo o seguinte comando:

```
install_dir/itm/config
```

5. Para ativar o rastreo do agente de monitoramento, certifique-se de que o valor está configurado no arquivo *sk\_agentInstance.config*:

```
KSK_TRACE='1'
```

Você também deve garantir que o seguinte valor esteja configurado no arquivo de configuração *sk.ini*:

```
KSK_TRACE=1
```

6. Se um representante de Suporte IBM solicitar que você ative rastreo para a API, certifique-se de que o seguinte valor esteja configurado no arquivo *sk\_agentInstance.config*:

```
KSK_APITRACE='1'
```

Você também deve garantir que o seguinte valor esteja configurado no arquivo de configuração *sk.ini*:

```
KSK_APITRACE=1
```

7. Inicie as instâncias do agente do Tivoli Monitoring for Tivoli Storage Manager concluindo uma das seguintes etapas:

- A partir da linha de comandos, emita os seguintes comandos:

```
cd install_dir/itm/tables  
../bin/itmcmd agent -o instance_name start sk
```

- A partir da interface gráfica com o usuário de CandleManage, selecione cada agente de monitoramento, clique nele com o botão direito do mouse e selecione **Iniciar**.

## Resultados

Para revisar os resultados do rastreo, localize os arquivos de log no diretório */install\_dir/itm/logs/*.

O arquivo de log que contém as informações de rastreo tem o seguinte formato: *aaaapppptttt.log* e o rastreo da API tem o seguinte formato: *aaaappppttttDsmQuery.out*, em que:

*aaaa* é o nome da instância do agente

*pppp* é o número da porta do servidor

*tttt* é o registro de data e hora

Por exemplo:

*instancename15001111103143325000.log* e *hostname1500DsmQuery.out*

---

## Rastreando o Agente do Tivoli Monitoring for Tivoli Storage Manager em um Sistema Operacional Windows

### Windows

Usando o Tivoli Monitoring for Tivoli Storage Manager, você pode criar e configurar instâncias do agente que monitoram servidores IBM Spectrum Protect. Para ativar o rastreo dos agentes de monitoramento para servidores em execução nos sistemas operacionais Windows, pare todas as instâncias do agente, modifique o arquivo de configuração e reinicie as instâncias do agente.

### Sobre Esta Tarefa

Antes de ativar o rastreo, você também pode abrir a área de trabalho de log de Agente de Tivoli Enterprise Portal e o grupo de atributos Log de Agente e visualizar as atividades do agente. A área de trabalho Log do Agente contém informações sobre qualquer servidor IBM Spectrum Protect que possua uma instância de agente configurada para monitorá-la.

Conclua as seguintes etapas para ativar o rastreo:

### Procedimento

1. Pare as instâncias do agente de monitoramento concluindo as seguintes etapas:
  - a. No servidor Tivoli Monitoring, clique em **Iniciar > Todos os Programas > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.
  - b. Selecione cada instância do agente de monitoramento, clique com o botão direito do mouse e selecione **Parar**.
2. Localize o diretório no qual o arquivo de configuração está armazenado:  
`install_dir\itm\tmaitm6`

Por exemplo:

`C:\IBM\itm\tmaitm6`

3. Para ativar o rastreo do agente, certifique-se de que o seguinte valor esteja configurado no arquivo `kskenv_agentInstance`:  
`KSK_TRACE=1`
4. A interface de programação de aplicativos (API) também pode ser rastreada, mas não é necessário, a não ser que seja solicitado por um representante de Suporte IBM. Para ativar o rastreo para a API, certifique-se de que o seguinte valor está configurado no arquivo `kskenv_agentInstance`:  
`KSK_APITRACE=1`
5. Inicie as instâncias do agente do Tivoli Monitoring for Tivoli Storage Manager concluindo as seguintes etapas:
  - a. No servidor do Tivoli Monitoring, clique em **Iniciar > Todos os Programas > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.
  - b. Selecione cada agente de monitoramento, clique com o botão direito do mouse e selecione **Iniciar**.

### Resultados

Os resultados do rastreo estão localizados no mesmo diretório do arquivo de configuração:

`install_dir\itm\tmaitm6\logs`



Os resultados do rastreo da API estão localizados no seguinte diretório:

*install\_dir\itm\tmaitm6*

Por exemplo:

C:\IBM\itm\tmaitm6\logs

C:\IBM\itm\tmaitm6

O arquivo de log que contém as informações de rastreo tem o formato aaaapppptttt.log e o rastreo da API tem o formato aaaappppttttDsmQuery.out, em que:

*aaaa* é o nome da instância do agente

*pppp* é o número da porta do servidor

*tttt* é o registro de data e hora

Por exemplo:

instancename15001111103143325000.log e hostname1500DsmQuery.out



---

## Capítulo 8. Resolvendo Problemas de Armazenamento de Dados

Se você estiver tendo um problema com o armazenamento ou com a recuperação de dados, vários métodos estarão disponíveis para ajudá-lo a resolver o problema.

---

### Resolvendo Problemas de Dados Ilegíveis

Você pode receber dados ilegíveis durante processos de importação ou de replicação de nós relacionados a uma falta de conversão de página de códigos durante esses processos.

Se os servidores estiverem em execução em diferentes códigos de idioma, algumas informações nos bancos de dados ou saída do sistema podem se tornar ilegíveis. Caracteres inválidos podem ser exibidos, por exemplo, nas informações de contato para os nós do administrador e do cliente, e em descrições de domínios de política. Qualquer campo que é armazenado no conjunto de caracteres do servidor e que usa caracteres ASCII estendidos pode ser afetado.

Para resolver o problema, atualize os campos com os comandos **UPDATE** apropriados depois da operação de importação ou de replicação de nó.

---

### Verificando o Log de Atividades do Servidor para Resolver Problemas de Armazenamento de Dados

Verifique o log de atividades do servidor para obter outras mensagens que ocorrem 30 minutos antes e 30 minutos depois do momento do erro.

Emita o comando **QUERY ACTLOG** para verificar o log de atividades. Geralmente, outras mensagens que são emitidas podem oferecer informações adicionais sobre a causa do problema e como resolvê-lo.

---

### Verificando em HELP Mensagens Emitidas para um Problema de Armazenamento de Dados

Verifique em HELP mensagens emitidas pelo IBM Spectrum Protect.

As mensagens do IBM Spectrum Protect fornecem informações adicionais nas seções **Explicação**, **Ação do Sistema** ou **Resposta do Usuário** da mensagem. Geralmente, estas informações suplementares sobre a mensagem podem fornecer as etapas necessárias para resolver o problema.

---

## Recriando o Problema de Armazenamento de Dados

Se um problema puder ser facilmente ou consistentemente recriado, será possível isolar a causa do problema para uma sequência específica de eventos.

Os problemas de leitura ou gravação de dados podem estar relacionados à sequência, em termos das operações que estão sendo executadas, ou podem ser um erro ou falha de dispositivo subjacente.

Problemas típicos relacionados à sequência de eventos ocorrem para volumes sequenciais. Um exemplo seria quando um volume está sendo usado para um backup de cliente e esse volume é influenciado por uma restauração de dados de outro nó do cliente. Esta situação pode ocorrer como um erro na sessão de backup de cliente que foi solicitada. No entanto, essa sessão de backup de cliente poderá ser bem-sucedida se tiver sido tentada novamente ou se não foi solicitada em primeiro lugar.

---

## Resolvendo Erros de Armazenamento de Dados Relacionados à Leitura ou Gravação em um Dispositivo

Se houver um erro devido à leitura ou composição de dados a partir de um dispositivo, muitos sistemas e dispositivos registram informações em um arquivo de log de erros do sistema. Por exemplo, o arquivo `errpt` para AIX e o arquivo Log de Eventos para Windows.

Se um dispositivo ou volume usado pelo estiver relatando um erro para o arquivo de log de erros do sistema, esse erro provavelmente será de dispositivo. As mensagens de erro gravadas no arquivo de log de erros do sistema podem fornecer informações suficientes para resolver o problema.

---

## Alterando a Hierarquia de Armazenamento para Resolver Problemas de Armazenamento de Dados

A hierarquia de armazenamento inclui os conjuntos de armazenamentos definidos e os relacionamentos entre os conjuntos de armazenamentos no servidor.

As definições de conjunto de armazenamento também são usadas pelo agente de armazenamento. Se os atributos de um conjunto de armazenamento tiverem sido alterados, a mudança poderá afetar as operações de armazenamento e recuperação de dados. Revise as mudanças na hierarquia de armazenamento e nas definições do conjunto de armazenamentos. Emita o comando **QUERY ACTLOG** para ver o histórico de comandos ou as mudanças que podem afetar os conjuntos de armazenamento. Além disso, use os seguintes comandos **QUERY** para determinar se foi feita alguma mudança:

- **QUERY STGPOOL F=D**

Revise as configurações do conjunto de armazenamentos. Se um conjunto de armazenamentos for **UNAVAILABLE**, os dados nesse conjunto de armazenamentos não poderão ser acessados. Se um conjunto de armazenamentos for **READONLY**, os dados não poderão ser gravados nesse conjunto. Se essa for a situação, revise o porquê desses valores terem sido configurados e considere emitir o comando **UPDATE STGPOOL** para configurar o conjunto para **READWRITE**. Outra consideração é revisar o número de volumes utilizáveis que estão disponíveis para um conjunto de armazenamento de mídia sequencial.

- **QUERY DEVCLASS F=D**

Os conjuntos de armazenamentos podem ser influenciados por mudanças nas classes de dispositivo. Revise as configurações de classe de dispositivo dos conjuntos de armazenamento, incluindo as definições de biblioteca, unidade e caminho. Emita os comandos **QUERY LIBRARY**, **QUERY DRIVE** e **QUERY PATH** para obter os conjuntos de armazenamento de mídia sequencial.

---

## Alterando as Políticas do Servidor para Resolver Problemas de Armazenamento de Dados

Os atributos de política do servidor que estão diretamente relacionados ao armazenamento de dados são os destinos do grupo de cópias para grupos de cópias de backup e archive. De forma semelhante, a classe de gerenciamento, **MIGDESTINATION**, também impacta onde os dados são armazenados.

Revise as mudanças nas políticas de armazenamento do servidor. Emita o comando **QUERY ACTLOG** para visualizar o histórico de comandos ou mudanças que podem afetar as políticas de armazenamento. Além disso, use os seguintes comandos **QUERY** para determinar se foi feita alguma mudança:

- **QUERY COPYGROUP F=D**

Revise as configurações de **DESTINATION** para os grupos de cópias **TYPE=BACKUP** e **TYPE=ARCHIVE**. Revise também o "Destino de Migração" para classes de gerenciamento usadas por clientes HSM. Se os destinos do conjunto de armazenamento forem alterados e operações de leitura ou gravação de dados resultantes agora falharem, avalie as mudanças feitas e corrija o problema ou volte às configurações anteriores.

- **QUERY NODE F=D**

Designar um nó para um domínio diferente pode causar impacto nas operações de leitura e gravação desse cliente. Especificamente, o nó agora pode ir para destinos do conjunto de armazenamentos não apropriados, com base nos requisitos deste nó. Por exemplo, ele pode ser designado a um domínio que não possui nenhum destino do grupo de cópias **TYPE=ARCHIVE**. Se esse nó tentar alcançar os dados, ele falhará.

---

## Resolvendo um Problema de Backup ou Cópia de Armazenamento de Dados que Ocorre apenas com um Nó Específico

Se não for possível fazer backup ou copiar dados para um nó específico, isto indica que você pode não ter um conjunto de dados ativos listado em seus destinos ativos. Eles são especificados no domínio da política de nó.

Emita o comando **QUERY NODE *nodeName* F=D** para verificar se o nó que está armazenando os dados é autorizado. O comando **QUERY NODE** localiza o nome de domínio de política ao qual o nó está designado. Emita **QUERY DOMAIN *domain\_name***, em que *domain\_name* é a saída reunida do comando anterior **QUERY NODE**. Consulte o parâmetro **ACTIVEDESTINATION** para obter a lista de portas de dados ativos. Se o conjunto de dados ativos no qual você deseja armazenar dados não estiver na lista, emita o comando **UPDATE DOMAIN** para incluir o conjunto de dados ativos na lista.

---

## Resolvendo um Problema de Armazenamento de Dados que Ocorre apenas para um Volume Específico

Se ocorrerem problemas apenas para um volume de armazenamento específico, pode haver um erro com o próprio volume, caso o volume seja uma mídia sequencial ou DISCO.

Se sua operação for uma operação de gravação de dados, emita o comando `UPDATE VOLUME volumeName ACCESS=READONLY` para configurar este volume como READONLY e, em seguida, tente novamente a operação. Se a operação for bem-sucedida, tente configurar o volume original de volta para READWRITE, emitindo o comando `UPDATE VOLUME volumeName ACCESS=READWRITE`. Tente novamente a operação. Se a operação falhar apenas ao usar este volume, será recomendável emitir o comando **AUDIT VOLUME** para avaliar este volume e emitir o comando **MOVE DATA** para mover dados deste volume para outros volumes no conjunto de armazenamentos. Quando os dados forem movidos para fora deste volume, exclua o volume emitindo o comando **DELETE VOLUME**.

---

## Sugestões e Dicas de Armazenamento

As sugestões e dicas reunidas aqui são de experiências de problemas reais. Você pode achar que uma das soluções é apropriada para corrigir o problema do IBM Spectrum Protect.

### Sugestões e Dicas do Driver de Dispositivo

Problemas com o driver de dispositivo podem ser atribuídos ao sistema operacional, ao aplicativo que usa o dispositivo, ao firmware do dispositivo ou ao próprio hardware de dispositivo.

Sempre que for encontrado um problema no dispositivo, pergunte: “Algum item foi alterado?”

Se o firmware do adaptador foi alterado, esta mudança poderá fazer um dispositivo exibir falhas intermitentes ou persistentes. Tente reverter para uma versão anterior do firmware para verificar se o problema continua.

Se o cabeamento entre o computador e o dispositivo foi alterado, esta mudança geralmente causa falhas intermitentes ou persistentes. Verifique mudanças no cabeamento para determinar se estão corretas.

Um dispositivo pode exibir falhas intermitentes ou persistentes se o firmware do dispositivo tiver sido alterado. Tente reverter para uma versão anterior do firmware para verificar se o problema continua.

Para conexões SCSI, um pino torto no cabo SCSI no qual ele conecta-se ao computador (ou dispositivo) pode causar erros nesse dispositivo ou em qualquer dispositivo no mesmo barramento SCSI. Um cabo com um pino torto deve ser reparado ou substituído. De forma semelhante, os barramentos SCSI devem ser terminados. Se um barramento SCSI for terminado de maneira incorreta, os dispositivos no barramento poderão exibir problemas intermitentes ou os dados transferidos no barramento poderão estar ou parecer danificados. Verifique os terminadores do barramento SCSI para assegurar que estejam corretos.

**Lembre-se:** Se as informações de “dicas e sugestões” não resolverem adequadamente o problema do driver de dispositivo ou esta for a configuração

inicial dos drivers de dispositivo do sistema, verifique se os dispositivos de hardware são suportados. Consulte o Portal de suporte.

### **Ajustando-se a Mudanças no Sistema Operacional**

A manutenção do sistema operacional pode alterar níveis de kernel, drivers de dispositivo ou outros atributos de sistema que podem afetar um dispositivo.

De forma semelhante, o upgrade da versão ou release do sistema operacional pode causar problemas de compatibilidade de dispositivo. Se possível, reverta o sistema operacional para o estado anterior à falha do dispositivo. Se a reversão não for possível, verifique se existem atualizações do driver de dispositivo que podem ser necessárias, com base neste nível de correção, release ou versão do sistema operacional.

### **Ajustando-se a Mudanças no Adaptador HBA ou SCSI ao Conectar-se ao Dispositivo**

Um driver de dispositivo comunica-se com um determinado dispositivo através de um adaptador.

Se ele for um dispositivo conectado a fibre channel, o driver de dispositivo usará um adaptador de barramento de host (HBA) para se comunicar. Se o dispositivo estiver conectado a SCSI, o driver de dispositivo usará um adaptador SCSI para se comunicar. Em qualquer caso, se o firmware do adaptador foi atualizado ou o próprio adaptador foi substituído, o driver de dispositivo poderá ter problemas ao usar o dispositivo.

Trabalhe com o fornecedor do adaptador para verificar se ele está instalado e configurado corretamente. A lista a seguir mostra as outras possíveis etapas:

- Se o adaptador tiver sido alterado, tente voltar ao adaptador anterior para ver se o problema foi resolvido.
- Se outro hardware no computador foi alterado ou o computador foi aberto, reabra o computador e verifique se o adaptador está posicionado corretamente no barramento. Abrir e alterar outro hardware no computador pode afrouxar as placas e outras conexões do computador, o que pode causar problemas intermitentes ou falha total dos dispositivos ou de outros recursos do sistema.

### **Resolvendo uma Conexão com Cabo Solto**

Se uma conexão estiver solta do dispositivo para o cabo, ou do cabo para o dispositivo, podem ocorrer problemas com um dispositivo.

Verifique as conexões e verifique se as conexões de cabos estão corretas e firmes.

Para dispositivos SCSI, verifique se os terminadores SCSI estão corretos e se não existem pinos tortos no próprio terminador. Um barramento SCSI terminado incorretamente pode resultar em problemas difíceis com um ou mais dispositivos nesse barramento.

## Resolvendo Mensagens de Erro no Log de Erro de Sistema

Um dispositivo pode tentar relatar um erro para um log de erro de sistema.

A seguir, exemplos dos diversos logs de erro do sistema:

- **AIX** errpt
- **Windows** Log de eventos

Os logs de erro de sistema podem ser úteis, porque as mensagens e informações registradas podem ajudar a relatar o problema ou as mensagens podem incluir recomendações sobre como resolver o problema.

Verifique o log de erro apropriado e execute ações com base nas mensagens que são emitidas no log de erro.

## Suportando módulos de kernel Linux de 32 ou 64 bits para aplicativos de 32 ou 64 bits

**Linux**

Os módulos de kernel Linux controlam o modo de bit do driver de dispositivo genérico SCSI do Linux, todos os diferentes drivers do Adaptador de Barramento de Host (HBA) e outras configurações.

Todos estes módulos de kernel suportam somente aplicativos que possuem o mesmo modo de bit com módulos de kernel em execução. Em outras palavras, os módulos de kernel de 64 bits suportam somente aplicativos de 64 bits em sistemas Linux de 64 bits.

Se um aplicativo de 32 bits for executado em um sistema Linux de 64 bits e invocar um módulo de kernel de 64 bits, o aplicativo de 32 bits causará uma falha de segmentação do kernel. Uma falha de segmentação também ocorrerá se o aplicativo de 64 bits chamar um módulo de kernel de 32 bits em um sistema Linux de 32 bits.

Para evitar essas falhas de segmentação, certifique-se de que o modo de bit do módulo de kernel Linux e seus aplicativos sejam iguais, verificando se os aplicativos de 32 bits podem chamar somente módulos de kernel de 32 bits em sistemas Linux de 32 bits e aplicativos de 64 bits que podem chamar somente módulos de kernel de 64 bits em sistemas Linux de 64 bits.

## Executando um servidor IBM Spectrum Protect Linux na arquitetura x86\_64

**Linux**

Os sistemas operacionais Linux de 32 e 64 bits podem ser executados nos sistemas AMD64 e EM64T, que são sistemas de 64 bits.

Um servidor e um agente de armazenamento Linux de 64 bits do IBM Spectrum Protect podem ser executados somente em um sistema AMD64/EM64T com um sistema operacional Linux de 64 bits. De forma semelhante, um servidor e um agente de armazenamento Linux de 32 bits do IBM Spectrum Protect podem ser executados somente em um sistema AMD64/EM64T com um sistema operacional Linux de 32 bits.

Um servidor IBM Spectrum Protect de 64 bits que emite o comando **QUERY SAN** requer uma interface de programação de aplicativos (API) de adaptador de



barramento de host (HBA) de 64 bits em um sistema AMD64/EM64T. Se um sistema AMD64 estiver equipado com um HBA Qlogic, isso pode criar um problema porque, por padrão, o Qlogic fornece uma API de HBA de 32 bits somente no sistema AMD64. Deve-se instalar a API de HBA de 64 bits no sistema antes de emitir o comando **QUERY SAN** de 64 bits.

## Ajustando-se a Mudanças no Driver HBA em Kernels Linux 2.6.x

A mudança mais distinta para drivers HBA em kernels Linux 2.6.x é que todos os drivers possuem “ko” como um novo sufixo.

A lista a seguir mostra os nomes e locais de drivers em kernels 2.6.x:

### Adaptec

O driver (aic7xxx.ko) está localizado no diretório `/lib/modules/kernel-level/drivers/scsi/aic7xxx/`.

### Emulex

O driver (lpfc.ko) está localizado no diretório `/lib/modules/kernel-level/drivers/scsi/lpfc/`.

### Qlogic

Seus nomes de drivers são qla2xxx.ko, qla2100.ko, qla2200.ko, qla2300.ko, qla2322.ko e outros. Existe uma certa ordem para carregar os drivers HBA. O qla2xxx.ko é um driver base e deve ser carregado primeiro. Depois de carregar o driver qla2xxx.ko, o sistema deve então carregar o driver qla2300.ko se ele estiver equipado com uma placa Qla2300. Todos os drivers estão localizados no diretório `/lib/modules/kernel-level/drivers/scsi/qla2xxx/`.

## Ativando o Suporte a Vários LUNs em Kernels Linux

Linux

Para configurar dispositivos SCSI com vários LUNs em um sistema Linux, o kernel Linux deve ser configurado para ativar o suporte a vários LUNs.

No entanto, o suporte a vários LUNs em algumas distribuições Linux não é uma opção padrão e requer que os usuários incluam manualmente esta opção no kernel em execução. Execute as seguintes etapas para configurar e ativar o suporte a várias LUNs na arquitetura IA32:

1. Inclua um parâmetro em um arquivo de configuração do utilitário de carga de inicialização.
  - Para o utilitário de carga de inicialização LILO:
    - a. Inclua `append="max_scsi_luns=128"` no arquivo `/etc/lilo.conf`.
    - b. Execute lilo.
  - Para o utilitário de carga de inicialização GRUB:
    - a. Inclua `max_scsi_luns=128` após a lista de imagens do kernel no arquivo `/etc/grub.conf` para a distribuição RedHat.
    - b. Inclua `max_scsi_luns=128` após a lista de imagens do kernel no arquivo `/boot/grub/menu.1` para a distribuição SuSE.
2. Reinicie o sistema.

## Usando o IBM Spectrum Protect para executar um ddtrace no Linux

Linux

O driver de dispositivo intermediário pode ser rastreado ao emitir o comando **DDTRACE**.

Para ativar o rastreo, emita os comandos a seguir a partir do console do servidor ou cliente admin:

```
trace enable lpdd <outros nomes de classe de rastreo do servidor>
trace begin <nome do arquivo>
```

Selecione uma das três opções a seguir:

- ddtrace start librarydd tapedd (para rastrear a biblioteca e a unidade)
- ddtrace start librarydd (somente rastreo da biblioteca)
- ddtrace start tapedd (somente rastreo da unidade)

**Lembre-se:** **DDTRACEGET** e **DDTRACE END** não são necessários.

O rastreo do driver de dispositivo intermediário do IBM Spectrum Protect não pode ser ativado por meio do utilitário ddtrace.

### Atualizando as informações sobre o dispositivo para sistemas host em uma SAN dinâmica sem reiniciar

Quando os dispositivos em um ambiente SAN são alterados, as informações sobre esse ambiente alterado não são automaticamente enviadas para os sistemas host conectados à SAN.

Se as informações sobre o dispositivo não forem atualizadas nos sistemas host que estão conectados à SAN, os caminhos do dispositivo que foram definidos anteriormente não existirão mais. Se você usar as informações sobre o dispositivo existentes para definir caminhos de dispositivo, dados de backup ou de restauração, estas operações poderão falhar. Para evitar esses tipos de falhas, use um método diferente para cada sistema operacional para atualizar as informações sobre o dispositivo na SAN sem reiniciar os sistemas host.

AIX

Emita o comando **CFGMGR** para forçar o sistema operacional a se reconfigurar. Em seguida, execute o SMIT para reconfigurar os dispositivos do IBM Spectrum Protect.

Linux

Não há nenhum comando do sistema para reconfigurar o sistema operacional. Para varrer novamente barramentos SCSI e fibre channels, os drivers adaptadores correspondentes a esses adaptadores SCSI e adaptadores fibre channel devem ser descarregados e, em seguida, recarregado no kernel Linux. Após recarregar os drivers HBA, execute o utilitário **autoconf** ou o comando **TSMSCSI** para reconfigurar dispositivos do IBM Spectrum Protect no Linux. É possível emitir o comando **LSPCI** para saber qual adaptador SCSI e adaptador fibre channel estão disponíveis no sistema. O comando **RMMOD** descarrega um driver do kernel e o comando **MODPROBE** carrega um driver no kernel.

Tabela 14. Adaptadores HBA e drivers correspondentes para arquiteturas do Linux

Adaptadores HBA	Nome do driver HBA	Arquiteturas disponíveis
Adaptec 7892	aix7xxx	IA32, AMD64

Tabela 14. Adaptadores HBA e drivers correspondentes para arquiteturas do Linux (continuação)

Adaptadores HBA	Nome do driver HBA	Arquiteturas disponíveis
Qlogic 22xx	qla2200	IA32, AMD64
Qlogic 23xx	qla2300	IA32, AMD64
Qlogic 2362	qla2362	EM64T
Emulex	lpfcdd	IA32, iSeries, pSeries

## Configurando Opções de vários LUNs como “on” para Configurações de BIOS de Adaptec SCSI e de HBA Qlogic Fibre-Channel no Linux

Por padrão, os adaptadores Adaptec SCSI configuram a opção de vários números de unidade lógica (LUN) como “off” em suas BIOS, o que torna o driver do adaptador SCSI incapaz de analisar corretamente uma unidade SCSI com vários LUNs.

### Procedimento

A opção de vários LUNs deve ser ativada. Conclua as etapas a seguir para ligar várias opções LUN:

1. Pressione as teclas Ctrl e A ao mesmo tempo.
2. Selecione **Configuração de Dispositivo SCSI** na Configuração **Configurar/Visualizar Adaptador de Host**.
3. Altere de Não para Sim para o suporte a vários LUNs do Bios.

### Ativando a Opção de Ativação de Fita:

Por padrão, os adaptadores de barramento de host fibre Qlogic configuram a opção ativada por fita como off em suas BIOS, o que afeta a execução de alguns comandos SCSI em vários dispositivos de fita SCSI.

### Procedimento

A opção de ativação de fita deve ser ligada. Conclua as etapas a seguir para ligar a opção de ativação de fita.

1. Pressione as teclas Alt e Q ao mesmo tempo.
2. Selecione **Configurações Avançadas**.
3. Altere Desativar para Ativar para o Suporte a Fitas Fibre Channel.

## Sugestões e Dicas de Unidades de Disco Rígido e de Subsistemas de Disco

O servidor IBM Spectrum Protect precisa de unidades de disco rígido, subsistemas de disco, sistemas de arquivos adquiridos pelo fornecedor e sistemas de arquivos remotos para ser executado de uma maneira específica. A execução de uma forma específica permite que o IBM Spectrum Protect gerencie e armazene dados adequadamente, garantindo a integridade no próprio servidor.

As seguintes definições são fornecidas para ajudá-lo a entender melhor as unidades de disco rígido e subsistemas de disco:

### Unidade de disco rígido

Geralmente, um dispositivo de armazenamento de unidade de disco rígido

é instalado dentro de um computador específico e usado para armazenamento por um servidor IBM Spectrum Protect nesse computador.

### **Subsistema de disco**

Um subsistema de disco externo se conecta a um computador por meio de uma SAN (rede de área de armazenamento) ou de algum outro mecanismo. Geralmente, os subsistemas de disco ficam fora do computador com o qual eles estão conectados e podem estar bem próximos ou podem estar localizados muito longe. Estes subsistemas também podem ter algum método de armazenamento em cache dos pedidos de entrada/saída nos discos. Se os dados forem armazenados em cache, apesar de uma solicitação de bypass de cache, que pode ocorrer nos sistemas de arquivos remotos e em determinados subsistemas de disco, falhas de entrada/saída podem ocorrer. As falhas ocorrem devido a uma diferença entre o rastreamento do IBM Spectrum Protect e o que realmente reside em um sistema de arquivos. Os sistemas de arquivos remotos e subsistemas de disco que exibem estas características não são suportados. Os subsistemas de disco geralmente têm seu próprio software de configuração e gerenciamento. Um subsistema de disco deve relatar os resultados de forma síncrona.

O servidor pode definir unidades de disco rígido e subsistemas de disco usados pelo computador ou sistema operacional no computador no qual o IBM Spectrum Protect está instalado. Geralmente, uma unidade de disco rígido ou subsistema de disco é definido para o computador no qual o IBM Spectrum Protect está instalado como uma unidade ou um sistema de arquivos. Quando a unidade de disco rígido ou o subsistema de disco estiver definido para o sistema operacional, o IBM Spectrum Protect poderá usar este espaço, alocando um banco de dados, um log de recuperação ou um volume do conjunto de armazenamentos no dispositivo. O volume do IBM Spectrum Protect é semelhante a outro arquivo nessa unidade ou sistema de arquivos.

### **Ignorando o Cache Durante Operações de Gravação**

O banco de dados, o log de recuperação e os volumes do conjunto de armazenamento são abertos com as configurações adequadas do sistema operacional para exigir que dados gravem solicitações para efetuar bypass de qualquer cache e serem diretamente gravados no dispositivo.

Efetuando bypass do cache durante as operações de gravação, o IBM Spectrum Protect mantém a integridade dos atributos e dos dados do cliente. O bypass do cache é requerido. Se um evento externo, como uma falha de energia, fizer com que o servidor ou o computador no qual o servidor está instalado pare ou tenha uma interrupção enquanto o servidor está executando, os dados no cache poderão ou não ser gravados no disco. Se os dados do IBM Spectrum Protect no cache de disco não forem gravados com êxito no disco, as informações no banco de dados do servidor ou log de recuperação poderão não ser concluídas. Além disso, os dados que supostamente seriam gravados nos volumes do conjunto de armazenamento poderão ficar ausentes.

Unidades de disco rígido instaladas no computador no qual o servidor está instalado e em execução têm menos de um problema com o bypass do cache. Nesse caso, as configurações do sistema operacional usadas quando o IBM Spectrum Protect abre volumes nessa unidade de disco rígido geralmente gerenciam o comportamento do cache de forma apropriada e consideram o pedido para evitar o armazenamento em cache de operações de gravação.

Geralmente, o uso e a configuração do armazenamento em cache de subsistemas de disco é um problema maior porque os subsistemas de disco normalmente não recebem informações do sistema operacional sobre o bypass do cache para operações de gravação. Os subsistemas de disco também podem ignorar essas informações quando um volume é aberto. Portanto, o armazenamento em cache das operações de gravação de dados pode resultar no dano do banco de dados do servidor ou na perda de dados do cliente, ou ambos. Os problemas dependem de quais volumes do IBM Spectrum Protect estão definidos no subsistema de disco e da quantidade de dados perdidos no cache. Os subsistemas de disco devem ser configurados para não armazenar em cache operações de gravação quando um banco de dados, log de recuperação ou volume do conjunto de armazenamentos do IBM Spectrum Protect for definido nesse disco. Outra alternativa é usar o cache não volátil para o subsistema de disco. O cache não volátil emprega um backup de bateria ou algum outro tipo de esquema para permitir que o conteúdo do cache seja gravado no disco se ocorrer uma falha.

### **Movendo Dados Existentes para outros Volumes antes de Alterar ou Mover o Banco de Dados**

O tamanho e local dos volumes (arquivos) do conjunto de armazenamento do IBM Spectrum Protect não podem ser alterados depois de serem definidos e usados pelo servidor.

Se o tamanho for alterado ou o arquivo for movido, informações internas que o IBM Spectrum Protect usa para descrever o volume poderão não mais corresponder aos atributos reais do arquivo. Se você precisar mover ou mudar o tamanho de um volume do conjunto de armazenamentos do IBM Spectrum Protect, mova os dados existentes para outros volumes antes de alterar ou mover o banco de dados.

### **Mapeamento de Diretório FILE entre Agentes de Armazenamento e Servidores para Arquivos Compartilhados**

Os servidores e agentes de armazenamento do IBM Spectrum Protect podem acessar os mesmos dados em classes de dispositivo FILE, definindo um conjunto de diretórios a serem usados em uma definição de classe de dispositivo.

O nome de diretório em uma definição de classe de dispositivo FILE identifica o local em que o servidor coloca os arquivos que representam volumes de armazenamento para a classe de dispositivo. Ao emitir o comando **DEFINE DEVCLASS**, o servidor expande o nome do diretório especificado em seu formato completo, começando do diretório raiz.

É possível especificar um ou mais diretórios como o local dos arquivos que são usados na classe de dispositivo FILE. O local padrão é o diretório atualmente em funcionamento do servidor no momento da emissão do comando. É possível especificar os diretórios para AIX ou Linux.

Não especifique diversos diretórios a partir do mesmo sistema de arquivos, porque isso pode causar cálculos de espaço incorretos. Por exemplo, se os diretórios `/usr/dir1` e `/usr/dir2` estiverem no mesmo sistema de arquivos, a verificação de espaço considerará cada diretório como um sistema de arquivos separado. A verificação de espaço faz uma avaliação preliminar do espaço disponível durante operações de armazenamento. Se os cálculos de espaço estiverem incorretos, o servidor poderá ser confirmado em um conjunto de armazenamentos FILE, mas não poderá obter espaço, causando falha da operação. Se a verificação de espaço

for exata, o servidor poderá ignorar o conjunto FILE na hierarquia de armazenamento e usar o próximo conjunto de armazenamentos, se houver um disponível.

Se o servidor precisar alocar um volume utilizável, ele criará um novo arquivo no diretório ou diretórios especificados. (O servidor pode escolher qualquer um dos diretórios no qual criar novos volumes de trabalho.) Para otimizar o desempenho, certifique-se de que vários diretórios correspondam a volumes físicos separados.

Consulte a tabela a seguir para a extensão do nome do arquivo que é criado pelo servidor para volumes utilizáveis, dependendo do tipo de dados que estão armazenados.

*Tabela 15. Extensões de nome de arquivo para volumes utilizáveis*

Para volumes utilizáveis usados para armazenar estes dados:	A extensão do arquivo é:
Dados do cliente	.BFS
Exportar	.EXP
Backup de banco de dados	.DBV

Para cada agente de armazenamento que compartilha o acesso **FILE**, os **PATHs** definidos para cada **DRIVE** exibido ao agente de armazenamento devem fornecer acesso ao mesmo conjunto de diretórios. Quando os **PATHs** estiverem definidos, os diretórios para cada agente de armazenamento deverão corresponder em número e ordem aos diretórios, conforme listado na definição de classe de dispositivo no servidor. Se estas definições estiverem fora de sincronização, o agente de armazenamento talvez não possa acessar os volumes FILE, o que pode resultar em restauração de LAN bem-sucedidas e em falhas de montagem para operações de restauração sem a LAN.

## Sugestões e Dicas de Unidades e Bibliotecas de Fitas

Os problemas com unidades de fita e bibliotecas podem ser com o software do computador que está tentando usar o dispositivo, as conexões com o dispositivo ou o dispositivo.

Sempre que for encontrado um problema no dispositivo, pergunte: “Algum item foi alterado?” Existe algo suspeito no computador que está tentando usar o dispositivo? Ou observe o próprio dispositivo, especialmente se ele funcionava antes de uma determinada mudança e depois parou.

- Se o firmware do adaptador foi alterado, um dispositivo pode exibir falhas intermitentes ou persistentes. Tente reverter para uma versão anterior do firmware para verificar se o problema continua.
- Se o cabeamento entre o computador e o dispositivo foi alterado, poderão ocorrer falhas intermitentes ou persistentes. Verifique mudanças no cabeamento para determinar se estão corretas.
- Se o firmware do dispositivo foi alterado, um dispositivo poderá exibir falhas intermitentes ou persistentes. Tente reverter para uma versão anterior do firmware para verificar se o problema continua.

## **Ajustando-se a Mudanças no Sistema Operacional**

A manutenção do sistema operacional pode alterar níveis de kernel, drivers de dispositivo ou outros atributos de sistema que podem afetar um dispositivo. De forma semelhante, o upgrade da versão ou release do sistema operacional pode causar problemas de compatibilidade de dispositivo.

Se possível, reverta o sistema operacional para o estado anterior à falha do dispositivo. Se a reversão do sistema operacional não for possível, verifique as atualizações do driver de dispositivos que possam ser necessárias, com base no nível de correção, liberação ou versão do sistema operacional.

## **Ajustando-se a Mudanças no Driver de Dispositivo**

Uma atualização de driver de dispositivo pode resultar no não funcionamento da unidade de fita ou dispositivo de biblioteca. Estes problemas também podem ocorrer como resultado do tipo de driver usado.

Ao trabalhar com bibliotecas ou unidades do IBM, em oposição ao uso de bibliotecas e unidades de outro fornecedor, o tipo de driver de dispositivo escolhido será importante. As bibliotecas e unidades do IBM devem usar o driver de dispositivo do IBM, enquanto as bibliotecas e unidades de outro fornecedor devem usar o driver de dispositivo do IBM Spectrum Protect.

Reverta para a versão anterior (ou mais antiga) do driver de dispositivo para verificar se o problema foi introduzido pela versão mais recente do driver.

## **Ajustando-se a um Adaptador Substituído ou a Outras Mudanças no Hardware**

Uma conexão Small Computer System Interface (SCSI) com o dispositivo usa um adaptador SCSI. Uma conexão fibre channel (ótica) com o dispositivo usa um adaptador de barramento de host (HBA).

Nos dois casos, a causa do problema pode ser proveniente de um adaptador alterado ou de um computador aberto no qual outro hardware foi alterado ou corrigido.

**Lembre-se:** O ponto de conexão do dispositivo com o computador é conhecido como um adaptador. Outro termo para adaptador é *placa*.

Consulte as informações a seguir para ajudar a ajustar-se a um adaptador ou hardware substituído:

- Se o adaptador tiver sido alterado, volte ao adaptador anterior para ver se o problema foi resolvido.
- Se o hardware no computador tiver sido alterado ou o computador estiver aberto, verifique-o para garantir que o adaptador esteja corretamente posicionado no barramento. Abrir e alterar outro hardware no computador pode afrouxar as placas e outras conexões do computador. O afrouxamento de conexões pode causar problemas intermitentes ou falha total dos dispositivos ou de outros recursos do sistema.

## Resolvendo uma Conexão com Cabo Solto

Podem ocorrer problemas com o dispositivo se uma conexão estiver solta do computador com o cabo, ou do cabo com o dispositivo.

Verifique as conexões e verifique se as conexões de cabos estão corretas e firmes.

Para dispositivos SCSI, verifique se os terminadores SCSI estão corretos e se não existem pinos tortos no próprio terminador. Um barramento SCSI terminado incorretamente pode resultar em problemas com um ou mais dispositivos nesse barramento.

## Usando Mensagens de Erro para Resolver um Mau Funcionamento do Dispositivo

Um dispositivo pode relatar um erro para um log de erro de sistema no qual é possível tentar localizar a causa do problema.

Os exemplos de vários logs de erro de sistema são:

- errpt para AIX
- Log de Eventos para Windows

Os logs de erro de sistema podem ser úteis, porque as mensagens e informações registradas podem ajudar a relatar o problema ou as mensagens podem incluir recomendações sobre como resolver o problema. Verifique o log de erros apropriado e execute as ações recomendadas com base nas mensagens emitidas no log de erros.

## Dicas e Sugestões de SAN

Os problemas com uma SAN (rede de área de armazenamento) podem ser com o software do computador que está tentando usar o dispositivo, com as conexões com o dispositivo ou com o dispositivo.

Sempre que for encontrado um problema da SAN, pergunte: “Algum item foi alterado?” Qualquer tipo de mudança pode ser suspeito, do computador que está tentando usar o dispositivo ao próprio dispositivo, especialmente se o dispositivo funcionava antes de uma determinada mudança e depois parou.

Para entender melhor como diagnosticar problemas com uma SAN, revise as seguintes terminologias e abreviações típicas:

### Fibre channel

Fibre channel indica uma conexão de fibra ótica com um dispositivo ou componente.

### Adaptador de barramento de host

Um adaptador de barramento de host (HBA) é usado por um determinado computador para acessar uma SAN. Um HBA é semelhante à função de um adaptador de rede em relação a como ele fornece acesso a um computador para uma LAN (rede local) ou WAN (rede de longa distância).

**SAN** Uma SAN é uma rede de dispositivos compartilhados que geralmente são acessados usando fibra. Geralmente, uma SAN é usada para compartilhar dispositivos entre muitos computadores diferentes.



## Conheça a configuração de sua SAN

Entender a configuração da SAN é essencial nos ambientes SAN. Várias implementações da SAN possuem limitações ou requisitos sobre como os dispositivos são configurados e instalados.

As três configurações da SAN são ponto a ponto, de loop arbitrado e malha comutada.

### Ponto a Ponto

Os dispositivos são conectados diretamente ao Adaptador de Barramento de Host (HBA).

### Loop arbitrado

As topologias de loop arbitrado são topologias em anel e são limitadas em termos do número de dispositivos que são suportados no loop e do número de dispositivos que podem ser usados em um determinado momento. Em um loop arbitrado, apenas dois dispositivos podem comunicar-se ao mesmo tempo. Os dados que estão sendo lidos de um dispositivo ou gravados em um dispositivo são passados de um dispositivo no loop para outro, até atingir o dispositivo de destino. O principal fator de limitação em um loop arbitrado é que apenas dois dispositivos podem ser usados em um determinado momento.

### Malha comutada

Em uma SAN de malha comutada, todos os dispositivos na malha serão dispositivos nativos de fibra. Esta topologia possui as maiores largura de banda e flexibilidade, porque todos os dispositivos estão disponíveis para todos os HBAs através de algum caminho de fibra.

## Assegurando que seu HBA Funciona com sua SAN

O adaptador de barramento de host (HBA) é um dispositivo crítico para o funcionamento adequado de uma SAN. Os problemas que podem ocorrer com HBAs variam de configuração não apropriada a BIOS ou drivers de dispositivo desatualizados.

Para um determinado HBA, verifique os seguintes itens:

**BIOS** HBAs possuem um BIOS integrado que pode ser atualizado. O fornecedor de HBA tem utilitários para a atualização da BIOS no HBA. Periodicamente, os HBAs em uso na SAN devem ser verificados para determinar se existem atualizações do BIOS que devem ser aplicadas.

### Driver de dispositivo

Os HBAs usam drivers de dispositivo para funcionar com o sistema operacional para fornecer conectividade com a SAN. Geralmente o fornecedor fornece um driver de dispositivo para usar com seu HBA. De modo semelhante, o fornecedor fornece instruções e todas as ferramentas ou utilitários necessários para atualizar o driver de dispositivo. Periodicamente o nível do driver de dispositivo deve ser comparado ao que está disponível a partir do fornecedor e, se necessário, atualizado para selecionar as correções e suportes mais recentes.

### Configuração

Os HBAs possuem diversas definições configuráveis. As configurações geralmente afetam como o IBM Spectrum Protect funciona com um dispositivo SAN.

### Referências relacionadas:

“Problemas de Configuração do HBA” na página 192

## Problemas de Configuração do HBA

Adaptadores de barramento de host (HBAs) possuem muitas definições e opções de configuração diferentes.

O fornecedor do HBA geralmente fornece informações sobre as configurações do seu HBA e dos valores adequados a essas configurações. De forma semelhante, o fornecedor do HBA pode oferecer um utilitário e outras instruções sobre como configurar seu HBA. As configurações a seguir geralmente afetam o uso do IBM Spectrum Protect com uma SAN:

- Topologia da Rede de Área de Armazenamento (SAN)

O HBA deve ser configurado adequadamente, com base na topologia da SAN usada atualmente. Por exemplo, se a SAN for um loop arbitrado, o HBA deverá ser definido para esta configuração. Se o HBA se conectar a um comutador, a porta deste HBA deverá ser configurada como “ponto a ponto” e não como “loop”.

Com o Mapeamento de Dispositivos SAN do IBM Spectrum Protect, é possível concluir a descoberta da SAN na maioria dos sistemas e a ligação persistente dos dispositivos não será necessária. Um servidor IBM Spectrum Protect poderá localizar o dispositivo, se o caminho do dispositivo foi mudado por causa de um reinício ou outro motivo.

Acesse o Portal de Suporte para verificar o suporte de nível de plataforma/fornecedor de HBA/driver para a descoberta de SAN do IBM Spectrum Protect.

- velocidade do link do Fibre Channel

Em muitas topologias da SAN, a SAN é configurada com uma velocidade máxima. Por exemplo, se a velocidade máxima do comutador Fibre Channel for de 1 GB/s, o HBA também deverá ser configurado como este mesmo valor. Ou o HBA deve ser configurado para negociação automática (AUTO), se ele suportar este recurso.

- O suporte de fita Fibre Channel está ativado?

O IBM Spectrum Protect requer que um HBA seja configurado com suporte a fitas. O IBM Spectrum Protect geralmente usa SANs para acesso a unidades e bibliotecas de fitas. Portanto, a configuração do HBA para suportar fitas deve ser ativada.

AIX

Linux

Para ajudar na determinação de problema, é possível usar o módulo `dsmsanlist` para obter informações sobre dispositivos em uma rede de área de armazenamento (SAN). O módulo `dsmsanlist` é instalado por padrão quando o servidor IBM Spectrum Protect ou o agente de armazenamento do IBM Spectrum Protect é instalado.

## Problemas de Configuração do Comutador Fibre-channel

Um comutador fibre channel suporta muitas configurações diferentes. As portas no comutador devem ser configuradas de forma apropriada para o tipo de SAN que está sendo configurada e para os atributos da SAN.

O fornecedor para o comutador geralmente fornece informações sobre as definições e configuração apropriadas, com base na topologia da SAN que está sendo implementada. De forma semelhante, o fornecedor do comutador deve fornecer um utilitário e outras instruções sobre como configurá-lo. As seguintes configurações geralmente afetam como o IBM Spectrum Protect usa a SAN:

### Velocidade do link Fibre-channel

Em muitas topologias da SAN, a SAN é configurada com uma velocidade

máxima. Por exemplo, se a velocidade máxima do comutador fibre-channel for de 1 GB/s, o Adaptador de Barramento de Host (HBA) também deverá ser configurado como este mesmo valor. Ou o HBA deve ser configurado para negociação automática (AUTO) se o HBA suportar este recurso.

#### **Modo de porta**

As portas no comutador devem ser configuradas de forma apropriada para o tipo de topologia da SAN que está sendo implementada. Por exemplo, se a SAN for um loop arbitrado, a porta deverá ser configurada como FL\_PORT. Para outro exemplo, se o HBA estiver conectado a um comutador, as opções do HBA deverão ser configuradas como “ponto a ponto” e não como “loop.”

### **Configurações de Porta do Gateway de Dados**

Um gateway de dados em uma SAN converte fibre channel em SCSI para dispositivos SCSI conectados ao gateway.

Os gateways de dados são populares em SANs porque permitem o uso de dispositivos SCSI, portanto, é importante que as configurações de porta para um gateway de dados estejam corretas.

O fornecedor para o gateway de dados geralmente disponibiliza informações sobre as definições e configuração apropriadas, com base na topologia da SAN que está sendo implementada e nos dispositivos SCSI usados. De forma semelhante, o fornecedor pode oferecer um utilitário e outras instruções sobre como configurá-lo. As seguintes configurações podem ser usadas para o modo de porta fibre channel na porta conectada em um gateway de dados:

#### **Destino privado**

Apenas os dispositivos SCSI conectados ao gateway de dados são visíveis e utilizáveis a partir desta porta. Para os dispositivos SCSI disponíveis, o gateway apenas passa os quadros para um determinado dispositivo de destino. As configurações de porta de destino privado geralmente são usadas para loops arbitrados.

#### **Destino privado e inicializador**

Apenas os dispositivos SCSI conectados ao gateway de dados são visíveis e utilizáveis a partir desta porta. Para os dispositivos SCSI disponíveis, o gateway apenas passa os quadros para um determinado dispositivo de destino. Como um inicializador, este gateway de dados também pode iniciar e gerenciar operações de movimentação de dados. Especificamente, existem comandos SCSI estendidos que permitem a movimentação de dados adquiridos de fornecedor. Configurando uma determinada porta como inicializador, ela fica elegível para ser usada para pedidos SCSI de movimentação de dados adquiridos de fornecedor.

#### **Destino público**

Todos os dispositivos SCSI conectados ao gateway de dados, bem como outros dispositivos disponíveis da malha, são visíveis e utilizáveis a partir desta porta.

#### **Destino público e inicializador**

Todos os dispositivos SCSI conectados ao gateway de dados, bem como outros dispositivos disponíveis na malha, estão visíveis e podem ser usados a partir dessa porta. Como um inicializador, este gateway de dados também pode iniciar e gerenciar operações de movimentação de dados. Especificamente, existem comandos SCSI estendidos que permitem a movimentação de dados adquiridos de fornecedor. Configurando uma

determinada porta como inicializador, ela fica elegível para ser usada para pedidos SCSI de movimentação de dados adquiridos de fornecedor.

## **Configuração da SAN entre Dispositivos**

Os dispositivos em uma SAN, como um gateway de dados ou um comutador, geralmente fornecem utilitários que exibem o que esse dispositivo verá na SAN.

É possível usar estes utilitários para entender melhor e resolver problemas da configuração da SAN. O fornecedor do gateway de dados ou comutador geralmente fornece um utilitário para a configuração. Como parte deste utilitário de configuração, geralmente há informações como:

- Como este dispositivo está configurado
- Outras informações que este dispositivo vê na topologia da SAN (da qual ele faz parte)

É possível usar estes utilitários do fornecedor para verificar a configuração da SAN entre dispositivos:

### **Gateway de dados**

Um gateway de dados relata todos os dispositivos Fibre Channel e os dispositivos SCSI que estão disponíveis na SAN.

### **Comutador**

Um comutador relata informações sobre a malha SAN.

## **O Relatório de Erro de Link Fibre Channel**

A maioria dos dispositivos SAN fornece ferramentas de monitoramento que podem ser usadas para relatar informações sobre estatísticas de erros e desempenho.

O fornecedor do dispositivo deve fornecer o utilitário para monitoramento. Se uma ferramenta de monitoramento estiver disponível, geralmente ela relatará erros. Os seguintes erros aparecem com mais frequência:

### **Erro de CRC, erro de código 8b/10b e outros sintomas semelhantes**

Esses erros são recuperáveis onde a manipulação de erros geralmente é fornecida pelo firmware ou hardware. Na maioria dos casos, o método para recuperar o dispositivo é retransmitir o quadro com falha. O link fibre-channel ainda está ativo quando estes erros são encontrados. Os aplicativos que usam um dispositivo SAN que encontra este tipo de erro de link geralmente não estão cientes do erro, a menos que seja um erro sólido. Um erro sólido é um erro no qual a recuperação do firmware e do hardware não pode retransmitir com êxito os dados após tentativas repetidas. A recuperação desse tipo de erro geralmente é muito rápida e não causará degradação no desempenho do sistema.

### **Falha de link (perda de sinal, perda de sincronização, primitiva NOS recebida)**

Este erro indica que um link está de fato “interrompido” por um período de tempo. Provavelmente devido à falha de um conector da interface de gigabit (GBIC), de um adaptador da interface de mídia (MIA) ou de um cabo. A recuperação para este tipo de erro é disruptiva. Esse erro aparece no aplicativo usando o dispositivo SAN que encontrou essa falha de link. A recuperação está no nível de troca de comando e envolve o aplicativo e o driver de dispositivo para executarem uma reconfiguração no firmware e no hardware, o que causa degradação na execução do sistema até que a recuperação do link esteja concluída. Estes erros devem ser monitorados de forma rigorosa, pois geralmente afetam vários dispositivos SAN.

**Lembre-se:** Erros de link fibre channel geralmente são causados por uma ação do engenheiro de cliente (CE) em substituir um dispositivo SAN. Como parte da manutenção executada pelo CE para substituir ou reparar um dispositivo SAN, o cabo de fibra pode ser temporariamente desconectado. Se o cabo de fibra for desconectado, o horário e a duração do erro devem corresponder ao momento em que a atividade do serviço foi executada.

## Erros Comuns de Dispositivos SAN

Várias mensagens específicas da SAN podem ser emitidas quando você passa por problemas com dispositivos SAN de seu agente de armazenamento.

Consulte a Tabela 16 para os erros gerados para dispositivos SAN.

*Tabela 16. Erros Comuns de Dispositivos SAN*

Erro	Explicação
ANR8302E Erro de E/S na unidade <i>TSMDRIVE01 (/dev/mt9)</i> (OP=WRITE, Número do Erro=5, CC=205, KEY=FF, ASC=FF, ASCQ=FF, SENSE=**NONE**, Descrição= <i>Falha geral de SCSI</i> ). Consulte o Apêndice D no manual 'Mensagens' para a ação apropriada	<p>Esta mensagem geralmente é emitida para erros do dispositivo SAN. O CC=205 relata que o driver de dispositivo detecta um erro do adaptador SCSI. Se um dispositivo conectado por SAN encontrar uma reconfiguração de link que é causada por perda do link, ela será relatada de volta ao driver de dispositivo como um erro do adaptador SCSI.</p> <p>A causa subjacente deste erro é o evento que causou a reconfiguração do link devido à perda do link. O caminho para este dispositivo pode ser atualizado para ONLINE=NO emitindo o comando <b>UPDATE PATH</b>. Não configure o caminho como ONLINE=YES até que a causa para a reconfiguração do link seja isolada e corrigida.</p>
ANR8957E: <i>comando</i> : A detecção automática está DESLIGADA e o número de série relatado pela biblioteca não correspondia ao número de série na definição da biblioteca	<p>O Mapeamento de Dispositivos SAN do IBM Spectrum Protect encontrou um caminho para a biblioteca que relata um número de série diferente da definição do IBM Spectrum Protect atual para a biblioteca. O parâmetro <b>AUTODETECT</b> foi configurado como NO para o comando que impediu o servidor de atualizar o número de série da biblioteca.</p> <p>Determine o novo caminho e emita o comando <b>UPDATE PATH</b> para corrigir esse erro.</p>
ANR8958E: <i>comando</i> : A detecção automática está DESLIGADA e o número de série relatado pela unidade não correspondia ao número de série na definição da unidade	<p>O Mapeamento de Dispositivos SAN do IBM Spectrum Protect encontrou um caminho para uma unidade que relata um número de série diferente da definição do IBM Spectrum Protect atual para a unidade. O parâmetro <b>AUTODETECT</b> foi configurado como NO para o comando, que impede o servidor de atualizar o número de série para esta unidade.</p> <p>Determine o novo caminho e emita o comando <b>UPDATE PATH</b> para corrigir esse erro.</p>

Tabela 16. Erros Comuns de Dispositivos SAN (continuação)

Erro	Explicação
ANR8963E: Não é possível localizar o caminho para corresponder ao número de série definido para a unidade <i>driveName</i> na biblioteca <i>libraryName</i>	<p>O Mapeamento de Dispositivos SAN não pôde localizar um dispositivo SAN que foi definido anteriormente para o servidor. A causa mais provável para isto é que o próprio dispositivo foi removido ou substituído na SAN. As etapas a seguir podem resolver esse erro:</p> <ul style="list-style-type: none"> <li>• Dispositivo Removido Se o dispositivo foi removido da SAN, exclua as definições do servidor que se referem a este dispositivo. Emita o comando <b>QUERY PATH F=D</b> para determinar os caminhos que se referem ao dispositivo. Em seguida, emita o comando <b>DELETE PATH</b> para remover estes caminhos.</li> <li>• Dispositivo Substituído Um Dispositivo SAN foi substituído por um novo dispositivo como resultado de manutenção ou de um upgrade. Execute os seguintes procedimentos: <ul style="list-style-type: none"> <li>– Tente não excluir a definição da unidade ou do caminho da unidade depois de substituir a unidade.</li> <li>– Emita um dos seguintes comandos do servidor: <ul style="list-style-type: none"> <li>- <b>UPDate DRive &lt;libraryName&gt; &lt;driveName&gt; SERIAL=AUTODetect</b> Este comando força/registra o novo número de série no banco de dados do servidor. Como a unidade é substituída, o número do elemento permanece igual.</li> <li>- <b>UPDate PATH &lt;sourceName&gt; &lt;driveName&gt; SRCT=SERVER DESTT=DRIVE LIBRARY=&lt;libraryName&gt; DEVIce=xxxxx AUTODetect=Yes</b> Este comando força/registra o novo número de série no banco de dados. Como a unidade é substituída, o número do elemento permanece igual.</li> </ul> </li> <li>– Se a unidade ou caminho da unidade for excluído, redefina essa unidade nova, substituída. Você deve reiniciar o servidor IBM Spectrum Protect para que o mapeamento do número de série/número de elemento da biblioteca seja atualizado. Esse mapeamento ocorre apenas na inicialização.</li> </ul> </li> </ul> <p>Emita o comando <b>QUERY PATH F=D</b> para localizar caminhos que estão definidos no servidor que referenciam este dispositivo, em seguida, emita o seguinte comando para atualizar as informações de caminho: <b>UPDATE PATH AUTODetect=Yes</b></p>
ANR8972E: Não é possível localizar o número do elemento para a unidade <i>driveName</i> na biblioteca <i>libraryName</i>	<p>Se o parâmetro <b>ELEment</b> for configurado para <b>AUTODetect</b> ao definir a unidade, o IBM Spectrum Protect obterá automaticamente o número do elemento da unidade. No entanto, se a biblioteca não fornecer um mapa do número do elemento/número de série, esta mensagem será emitida.</p> <p>Execute as seguintes etapas para corrigir esse erro:</p> <ol style="list-style-type: none"> <li>1. Determine o número do elemento para esta unidade de fita.</li> <li>2. Emita o comando <b>UPDATE DRIVE</b> para atualizar o número do elemento do dispositivo.</li> </ol>

**AIX** **Linux** Para ajudar na determinação de problema, é possível usar o módulo `dsmsanlist` para obter informações sobre dispositivos em uma rede de área de armazenamento (SAN). O módulo `dsmsanlist` é instalado por padrão quando o servidor IBM Spectrum Protect ou o agente de armazenamento do IBM Spectrum Protect é instalado.

**Conceitos relacionados:**

“Erros de Mapeamento de Dispositivos SAN” na página 198

## **Sugestões e Dicas de Mapeamento de Dispositivos SAN**

A descoberta de dispositivo SAN e o mapeamento de dispositivo são suportados no Windows, AIX e Linux (exceto o Linux zSeries).

Os itens a seguir ilustram as vantagens da descoberta de dispositivos e do mapeamento de dispositivos SAN do IBM Spectrum Protect:

### **O IBM Spectrum Protect pode exibir todos os dispositivos na SAN**

O comando do servidor **QUERY SAN** mostra todos os dispositivos que são vistos pelo servidor via todos os adaptadores de barramento de host (HBAs) Fibre Channel no sistema. Os parâmetros mostrados são tipo de dispositivo, nome do fornecedor, nome do modelo do produto, número de série e nome do dispositivo. Se `FORMAT=DETAIL` for especificado para a consulta, informações adicionais, tais como, World Wide Name (WWN), porta, barramento, destino e LUN são exibidas. As informações ajudam a identificar todas as fitas, discos e dispositivos movedores de dados no SAN. Para AIX, o movedor de dados não é aparente e não é mostrado.

### **O IBM Spectrum Protect pode atualizar o caminho do dispositivo automaticamente quando um caminho de dispositivo é alterado**

O IBM Spectrum Protect não exige ligação persistente para os dispositivos que ele vê por meio do HBA. Ao contrário, o servidor usa o SNIA (Storage Networking Industry Association) HBAAPI para descobrir e obter o número de série de todos os dispositivos na SAN. Ele também pode determinar cada caminho do dispositivo. Ao comparar um número de série do dispositivo que é registrado no banco de dados IBM Spectrum Protect com o número de série obtido do dispositivo em tempo real, uma mudança em um caminho do dispositivo é detectada. Se o caminho tiver sido alterado, a descoberta da SAN obterá automaticamente o novo caminho para o dispositivo. O banco de dados do IBM Spectrum Protect também é atualizado com as informações do novo caminho.

A biblioteca de wrapper HBAAPI é o wrapper usado pelo servidor para se comunicar com o SNIA HBAAPI. A biblioteca de wrapper HBAAPI é instalada no mesmo diretório que o arquivo executável do IBM Spectrum Protect (a menos que o caminho completo seja especificado). A lista a seguir mostra os arquivos de wrapper HBA incluídos com o pacote do servidor (exceto no AIX):

- **Windows** `hbaapi.dll`
- **AIX** `/usr/lib/libhbaapi.a` (fornecido pelo AIX com a instalação HBAAPI)
- **Linux** 32 bits: `libhbaapi32.so`
- **Linux** 64 bits: `libhbaapi64.so`

Se um desses arquivos estiver ausente, a mensagem “ANR1791W A biblioteca do wrapper HBAAPI xxxxxxxx falhou ao carregar ou está ausente.” será exibida. A mensagem será exibida.

### **Desativando o Mapeamento de Dispositivos SAN:**

Ocasionalmente, você deve desativar o mapeamento de dispositivo SAN para contornar ou isolar um problema quando estiver resolvendo problemas com o dispositivo.

### **Sobre Esta Tarefa**

Execute as seguinte etapa para desativar o mapeamento de dispositivos e a descoberta de dispositivos SAN:

### **Procedimento**

Emita o comando do servidor **setopt SANDISCOVER OFF**. Os comandos **setopt SANDISCOVERY** podem ser emitidos quantas vezes forem necessárias.

**Dica:** Outra maneira de desativar/ativar a descoberta da SAN é inserir a seguinte opção no arquivo dsm serv.opt:

**SANDISCOVERY OFF** desativa a descoberta da SAN.

**SANDISCOVERY ON** ativa a descoberta da SAN.

**SANDISCOVERY ON** é o padrão para as plataformas AIX, Linux e Windows.

### **Informações Específicas da Plataforma:**

Ao trabalhar com seu mapeamento de dispositivo SAN, é importante que você saiba as informações específicas da sua plataforma.

**AIX** O comando **QUERY SAN** não mostra nenhum dispositivo de Gateway, pois os dispositivos de Gateway não são aparentes para o AIX.

**Linux** Existem bibliotecas, utilitários e outros itens separados para RHEL3U3. Para executá-los, você deve também instalar um módulo de kernel ioctl Emulex além do driver Emulex. Certifique-se de ter carregado o driver Emulex antes de carregar o módulo ioctl.

**Dica:** Consulte a lista de HBAs suportados e níveis de driver requeridos pelo sistema operacional.

### **Erros de Mapeamento de Dispositivos SAN**

Os erros que são gerados com mais frequência durante o mapeamento de dispositivo SAN podem estar relacionados à descoberta SAN, ao mau funcionamento do dispositivo SAN, às bibliotecas que não são válidas e a outros problemas relacionados à SAN.

**ANR1745I: Não é possível descobrir dispositivos SAN. A função está ocupada.**

Esta mensagem de erro aparecerá se houver outra descoberta da SAN ativa.

O servidor não pode executar a descoberta de SAN. Tente novamente após a conclusão da descoberta da outra SAN.



## **ANR1786W, ANR1787W ou ANR1788W**

Você pode ver mensagens de erro ANR1786W, ANR1787W ou ANR1788W quando há um problema com a descoberta da SAN. As três mensagens a seguir geralmente indicam que a biblioteca HBAAPI não está funcionando em geral:

- ANR1786W HBAAPI não consegue obter o nome do adaptador
- ANR1787W Não é possível abrir o adaptador *adaperName*
- ANR1788W Não é possível obter os atributos do adaptador para *adapterName*

Se o resultado for que o servidor não pode executar a descoberta de SAN, vá para o Portal de suporte para verificar se o driver adaptador de barramento de host (HBA) está atualizado e em um nível suportado.

## **ANR1789W Falha ao Obter o Mapeamento de Destino HBA**

A mensagem de erro ANR1789W é o erro HBAAPIn mais comum na SAN.

“Falha ao obter o mapeamento de destino HBA” significa que o HBA encontrou um erro ao reunir informações de mapeamento de dispositivos enviando vários comandos SCSI.

Verifique se todos os dispositivos SAN estão funcionando corretamente (por exemplo, um Gateway de Dados da SAN pode ser interrompido e talvez precise ser reinicializado). Se todos os dispositivos parecerem funcionais, verifique se o firmware do dispositivo na SAN, e o driver HBA, estão nos níveis apropriados. Se o resultado for que o servidor não pode executar a descoberta de SAN, vá para Portal de suporte para verificar se o driver HBA está atualizado e em um nível suportado.

**Dica:** Para dispositivos de fita IBM, certifique-se de que o firmware mais recente esteja instalado. O firmware anterior ao 4772 para dispositivos de fita 3580 IBM causa problemas com o Qlogic HBAAPI.

## **ANR1790W Falha na Descoberta da SAN**

A mensagem de erro ANR1790W é uma mensagem geral que indica que a função HBAAPI falhou e não pode executar a descoberta da SAN.

Verifique se todos os dispositivos SAN estão funcionando corretamente (por exemplo, um Gateway de Dados da SAN pode ser interrompido e talvez precise ser reinicializado). Se todos os dispositivos parecerem funcionais, verifique se o firmware do dispositivo na SAN, e o driver HBA, estão nos níveis apropriados.

**Dica:** Para dispositivos de fita IBM, certifique-se de que o firmware mais recente esteja instalado. O firmware anterior ao 4772 para dispositivos de fita 3580 IBM causa problemas com o Qlogic HBAAPI.

## **ANR1791W A biblioteca de wrapper xxxxx HBAAPI falhou ao carregar ou está ausente**

A biblioteca de wrapper HBAAPI é usada pelo servidor para se comunicar com o SNIA HBAAPI.

As bibliotecas de wrapper HBAAPI estão no mesmo diretório que o arquivo executável do IBM Spectrum Protect (a menos que o caminho completo seja fornecido conforme mostrado abaixo). A lista a seguir mostra os arquivos de

wrapper HBA que são enviados com o pacote do servidor (exceto no AIX e Linux zSeries). A mensagem de erro ANR1791W indica que o arquivo wrapper HBAAPI está ausente ou não pode ser carregado pelo IBM Spectrum Protect. Verifique se o arquivo wrapper está no mesmo diretório que o arquivo executável do IBM Spectrum Protect. Os arquivos da biblioteca do wrapper HBAAPI são mostrados na lista a seguir:

- **Windows** hbaapi.dll
- **AIX** /usr/lib/libhbaapi.a (fornecido pelo AIX com a instalação HBAAPI)
- **Linux** 32 bits: libhbaapi32.so
- **Linux** 64 bits: libhbaapi64.so

O resultado é que o servidor não pode executar a descoberta de SAN.

### **ANR1792W A biblioteca do fornecedor HBAAPI falhou ao carregar ou está ausente**

A mensagem de erro ANR1792W indica que o arquivo de biblioteca do fornecedor falhou ao carregar. Verifique a validade dos arquivos de biblioteca.

Os sistemas AIX ou Linux (exceto no Linux zSeries) armazenam suas bibliotecas HBAAPI no local especificado pelo arquivo /etc/hba.conf. Arquivos Windows são armazenados no diretório C:\winnt\system32. Os seguintes exemplos são de arquivos de biblioteca do fornecedor:

- C:\winnt\system32\qlsdm.dll (arquivo do Windows de QLogic)
- /usr/lib/libHBAAPI.a (arquivo do AIX de Emulex)
- /usr/lib/libqlsdm.so (arquivo do Linux de Qlogic)
- /usr/lib/libemulexhbaapi.so (arquivo do Linux de 32 bits de Emulex)
- /usr/lib64/libemulexhbaapi.so (arquivo do Linux de 64 bits de Emulex)

O resultado é que o servidor não pode executar a descoberta de SAN.

### **ANR1793W A Descoberta da SAN do IBM Spectrum Protect Não É Suportada nesta Plataforma ou nesta Versão do S.O.**

A mensagem de erro ANR1793W será exibida apenas se o IBM Spectrum Protect tentar uma operação de mapeamento de dispositivos ou de descoberta de dispositivos SAN em um sistema operacional não suportado. Os seguintes sistemas operacionais não são atualmente suportados pelo mapeamento de dispositivo SAN ou pela descoberta de dispositivos:

- Windows 2003 de 64 bits
- Versões do AIX que não são 52L ou 53A. O suporte para o mapeamento de dispositivos e descoberta de dispositivos SAN no AIX requer a versão 52L (nível do conjunto de arquivos de 5.2.0.50) ou 53A (nível do conjunto de arquivos 5.3.0.10) ou superior.

O resultado é que o servidor não pode executar a descoberta de SAN.

### **ANR1794W A descoberta da SAN do IBM Spectrum Protect foi desativada por opções**

A mensagem de erro ANR1794W indica que a descoberta de SAN no servidor está desativada.

A descoberta da SAN pode ser desativada ou ativada emitindo os seguintes comandos do servidor:

**setopt SANDISCOVERY OFF e setopt SANDISCOVERY PASSIVE**

Esses dois comandos desativam a descoberta da SAN. O servidor não pode corrigir o caminho do dispositivo automaticamente se o caminho tiver sido mudado. Esse comando precisa ser emitido apenas uma vez.

A diferença entre os dois comandos é que **SANDISCOVERY OFF** pesquisa o dispositivo e marca o caminho inativo como offline. **SANDISCOVERY PASSIVE** não pesquisa o dispositivo e não marca o caminho inativo como offline.

**setopt SANDISCOVERY ON**

Este comando ativa a descoberta da SAN. O comando **SETOPT SANDISCOVERY ON** pode ser emitido quantas vezes forem necessárias.

Outra maneira de desativar/ativar a descoberta da SAN é colocar a seguinte opção no arquivo `dsmserv.opt`:

**SANDISCOVERY OFF ou SANDISCOVERY PASSIVE**

Esses dois comandos podem desativar a descoberta da SAN.

**SANDISCOVERY ON**

Este comando ativa a descoberta da SAN.

AIX

Linux

Windows

**SANDISCOVERY** é padronizado como ON.

Vá para o Portal de suporte para verificar o nível de suporte da plataforma/fornecedor HBA/nível de driver antes de configurar **SANDISCOVERY ON** para ativar a descoberta de SAN.

AIX

Linux

Para ajudar na determinação de problema, é possível usar o módulo `dsmsanlist` para obter informações sobre dispositivos em uma rede de área de armazenamento (SAN). O módulo `dsmsanlist` é instalado por padrão quando o servidor ou o agente de armazenamento é instalado.

**ANR2034E QUERY SAN: Não foi localizada nenhuma correspondência usando estes critérios**

A mensagem de erro ANR2034E é emitida quando o servidor tenta coletar informações de configuração para SAN e não encontra nada.

O resultado é que o servidor não pode executar a descoberta de SAN.

A seguir, razões possíveis para não localizar informações sobre a SAN:

- O nível de sistema ou S.O. não é suportado.
- Este ambiente não é um ambiente SAN.
- Pode haver um problema com a SAN.
- O HBA API pode retornar o valor zero do número de HBAs no sistema.
- O HBA API pode retornar o valor zero do número de dispositivos no sistema.

Execute as seguintes tarefas para localizar as informações de configuração da SAN:

- Verifique o driver HBA fibre-channel e certifique-se de que ele esteja instalado e ativado.
- Verifique o nível de driver HBA para assegurar que ele esteja atualizado.

- Use a capacidade do fornecedor HBA para verificar quaisquer problemas de link fibre-channel relatados.
- Desinstale e, em seguida, instale o driver HBA. Se houver um problema com a configuração do HBA, o driver de dispositivo ou de compatibilidade, às vezes desinstalar e reinstalá-lo corrige o problema.
- Verifique a conexão do cabo fibre-channel com o HBA.
- Verifique a conexão do cabo fibre-channel do HBA com o dispositivo SAN (comutador, gateway de dados ou outro dispositivo).
- Verifique o Gigabit Inter-phase Converter (GBIC).
- No dispositivo SAN (comutador, gateway de dados ou outro dispositivo), tente uma porta de destino diferente. Às vezes, os dispositivos SAN podem ter uma falha de porta específica.
- Pare o servidor, reinicie o sistema e reinicie o servidor. Se houver mudanças na configuração na SAN, às vezes o sistema operacional, driver de dispositivo ou HBA requer uma reinicialização do sistema antes de se comunicar com a SAN.
- Recicle a porta de destino no dispositivo SAN.
- Reconecte a placa HBA.
- Reconecte o HBA.

### **ANR8226E Erro ao Detectar Versão da Biblioteca HBA-API**

A mensagem de erro ANR8226E é exibida apenas para o AIX.

O servidor tentou determinar o nível do conjunto de arquivos `devices.common.IBM.fc.hba-api` fileset e encontrou um erro. A mensagem de erro ANR8226E indica que ocorreu um erro ao tentar detectar a versão da biblioteca HBA-API no AIX.

O resultado é que o servidor não pode executar a descoberta de SAN.

AIX

### **ANR8227E O conjunto de arquivos `devices.common.IBM.fc.hba-api` não está no nível necessário**

Devido a problemas no código HBAAPI do AIX, os níveis mínimos de `devices.common.IBM.fc.hba-api` do conjunto de arquivos necessários para a recuperação bem-sucedida da SAN são mostrados na lista a seguir:

- AIX52 - Necessário 5.2.0.50
- AIX53 - Necessário 5.3.0.10

O servidor especificou que o conjunto de arquivos `devices.common.IBM.fc.hba-api` está em um nível incompatível com operações do IBM Spectrum Protect. Instale a manutenção mais recente para este conjunto de arquivos, se você usar dispositivos SAN.

O resultado é que o servidor não pode executar a descoberta de SAN.

#### **Referências relacionadas:**

“Sugestões e Dicas de Mapeamento de Dispositivos SAN” na página 197

## Os Dispositivos SAN Estão Ausentes da Exibição do Comando do Servidor QUERY SAN:

As possíveis razões para o comando do servidor **QUERY SAN** não mostrar todos os dispositivos podem ser devido a problemas de configuração ou de suporte do fornecedor.

Assegure-se de que a opção do servidor SANDISCOVERY esteja configurada como ON.

*Atualizando a Configuração da SAN:*

O comando do servidor **QUERY SAN** pode não exibir todos os dispositivos devido à configuração da SAN.

Pode ser necessário atualizar a SAN porque a configuração foi alterada (incluir/remover dispositivo) e a configuração do sistema precisa ser atualizada.

### Atualizar configuração no AIX:

#### Para dispositivos IBM:

Emita o comando **cfgmgr** para configurar novos dispositivos e visualizar a nova configuração. O nome do arquivo especial para dispositivos de fita IBM (não os dispositivos IBM Spectrum Protect) é /dev/rmtX para unidades de fita e /dev/smcX para dispositivos de troca médios.

**Dica:** Nome do arquivo especial: /dev/rmt0, /dev/smc0

#### Para dispositivos IBM Spectrum Protect:

Para atualizar os arquivos especiais, use **smitty > dispositivos > Dispositivos IBM Spectrum Protect > remover todos os dispositivos definidos**, em seguida, **descobrir dispositivos suportados pelo IBM Spectrum Protect**. O nome do arquivo especial é /dev/mtX para unidades de fita e /dev/lbX para dispositivos de troca médios.

**Dica:** Nome do arquivo especial: /dev/mt0, /dev/lb0

Como alternativa, é possível reinstalar o driver de dispositivo da IBM. O driver de dispositivo IBM Spectrum Protect atualiza todos os nomes de arquivos especiais atuais.

### Atualizar configuração no Windows:

Com o plug and play, o registro do Windows é atualizado e o nome do dispositivo pode ser alterado sem a necessidade de reiniciar o computador ou sem a participação do driver de dispositivo. O servidor IBM Spectrum Protect detecta a mudança em um nome do arquivo especial e atualiza o novo nome do arquivo especial quando acessa os dispositivos de fita (durante a inicialização do servidor ou operação normal). O nome do dispositivo correto é atualizado no banco de dados do IBM Spectrum Protect. O nome do arquivo especial é /dev/mtA.B.C.D para dispositivos IBM Spectrum Protect e dispositivos IBM; e /dev/lbA.B.C.C para dispositivos IBM Spectrum Protect e dispositivos de troca médios IBM. O nome do arquivo especial TapeX é somente para as unidades de fita IBM e ChangerX é somente para os dispositivos de troca médios IBM.

**Dica:** Nome do arquivo especial: mt0.1.0.0, lb0.0.1.0, Tape0, e Changer0.

## Atualizar configuração no Linux:

O Adaptador de Barramento de Host (HBA) obtém as informações de configuração mais recentes como resultado do RSCN. Às vezes, o computador deve ser reiniciado para poder efetivar as alterações na configuração.

### Para dispositivos IBM:

Emita o comando **lin\_taped** para reconfigurar os dispositivos. As informações sobre o dispositivo podem ser recuperadas a partir do arquivo `/proc/scsi/IBMtape` para dispositivos de fita e do arquivo `/proc/scsi/IBMchanger` para dispositivos de troca médios. O nome do arquivo especial é `/dev/IBMTapeX` para dispositivos de fita e `/dev/IBMChangerX` para dispositivos de troca médios.

**Dica:** Nome do arquivo especial: `/dev/IBMTape0`,  
`/dev/IBMChanger0`

### Para dispositivos IBM Spectrum Protect:

Os usuários podem emitir `autoconf`, o script de configuração automática do driver de dispositivo IBM Spectrum Protect. Esse script reside no diretório `/opt/tivoli/tsm/devices/bin` (ou no mesmo diretório que o arquivo `tsmscsi`) para poder configurar os dispositivos e obter todos os nomes de arquivo especial atual e as informações sobre o dispositivo. O nome do arquivo especial do dispositivo é `/dev/mtX` para dispositivos de fita e `/dev/lbX` para dispositivos de troca médios.

**Dica:** Nome do arquivo especial: `dev/tsmscsi/mt0`,  
`/dev/tsmscsi/lb0`

Como alternativa, é possível reinstalar o driver de dispositivo da IBM. O driver de dispositivo IBM Spectrum Protect atualiza todos os nomes de arquivos especiais atuais.

Com o driver de dispositivo intermediário Linux para os dispositivos IBM Spectrum Protect, o driver HBA e o driver genérico devem ser recarregados para obter todos os nomes de arquivos especiais atuais. É necessário executar o script `autoconf` para que o driver de dispositivo IBM Spectrum Protect possa criar arquivos de configuração (`/dev/tsmscsi/lbinfo` e `/dev/tsmscsi/mtinfo`). Estes arquivos são usados pelo servidor IBM Spectrum Protect para criar os nomes de arquivos especiais após cada descoberta da SAN.

### 32 bits (Linux xSeries)

Certifique-se de que a biblioteca de wrapper HBAAPI `libhbaapi32.so` esteja no mesmo diretório que `dsmserv` ou no diretório `/opt/tivoli/tsm/server/bin`.

### 64 bits (Linux pSeries)

Certifique-se de que a biblioteca de wrapper HBAAPI `libhbaapi64.so` esteja no mesmo diretório que `dsmserv` ou no diretório `/opt/tivoli/tsm/server/bin`.

### 64 bits (Linux zSeries)

Certifique-se de que a biblioteca de wrapper pseudo-HBAAPI `libhbaapi64.so` esteja no mesmo diretório que `dsmserv` ou no diretório `/opt/tivoli/tsm/server/bin`. A biblioteca de wrapper, `libhbaapi64.so`, é um link para o arquivo `/usr/lib64/libzfcphbaapi.so`.

### *Resolvendo Problemas de Configuração que Causam Ausência do Dispositivo SAN:*

As possíveis razões para o comando do servidor **QUERY SAN** não exibir todos os dispositivos podem estar ligadas a problemas de configuração com o hardware HBA, nível de driver HBA ou nível de sistema operacional.

#### **Sobre Esta Tarefa**

Execute as seguintes etapas para resolver problemas de configuração:

#### **Procedimento**

1. Acesse o Portal de Suporte. Verifique o nível de suporte de nível de plataforma/fornecedor de HBA/driver para certificar-se de que o nível do driver HBA e o nível do sistema operacional sejam compatíveis e suportados pelo IBM Spectrum Protect para a descoberta do SAN.
2. Use o utilitário do fornecedor de HBA para verificar se o dispositivo pode ser visto pelo HBA. Se o dispositivo não for visto pelo HBA, o dispositivo não pode ser conectado. Verifique o cabo Fibre Channel ou SCSI. Se o dispositivo for visto pelo HBA, verifique a versão do driver HBA. Esta versão do driver pode ter problemas com a API HBA.
3. AIX Linux Use o módulo `dsmsanlist` para obter informações sobre dispositivos em uma rede de área de armazenamento (SAN). O módulo `dsmsanlist` é instalado por padrão quando o servidor IBM Spectrum Protect ou o agente de armazenamento do IBM Spectrum Protect é instalado.

### *Verificando o Suporte do Fornecedor para qualquer Dispositivo Específico na SAN:*

Muitos dispositivos ou combinações de dispositivos podem não ser suportados em uma determinada Rede de Área de Armazenamento (SAN). Estas limitações surgem da capacidade de um determinado fornecedor em certificar seu dispositivo usando um Protocolo Fibre Channel.

Para um determinado dispositivo, verifique com o fornecedor do dispositivo se ele é suportado em um ambiente da SAN. O suporte do fornecedor inclui todo o hardware associado à SAN, que significa verificar se este dispositivo é suportado com os fornecedores dos HBAs, hubs, gateways e comutadores que forma o ambiente da SAN.

## **Sugestões e Dicas de Operações do Arquivador NDMP para o Servidor IBM Spectrum Protect**

O IBM Spectrum Protect está padronizado para a porta de controle do protocolo de gerenciamento de dados de rede padrão (NDMP) 10000. Se esta porta estiver sendo usada por outro aplicativo (como um segundo servidor IBM Spectrum Protect), todas as operações o arquivador para o servidor falharão.

Para evitar conflitos com outros aplicativos, use a opção do servidor `NDMPCONTROLPORT` para especificar uma porta diferente para seu servidor.

Durante as operações de arquivador para servidor, o IBM Spectrum Protect usa os seguintes itens:

- Até duas portas TCP/IP adicionais.
- Uma porta de controle usada internamente pelo IBM Spectrum Protect durante as operações de backup e restauração.

- Uma porta de dados durante operações de backup de NDMP para um conjunto de armazenamentos nativos do IBM Spectrum Protect.

A porta de dados é uma porta efêmera que é adquirida no início de operações de backup de NDMP para um conjunto de armazenamentos nativos do IBM Spectrum Protect. Se uma porta não estiver disponível, será emitida uma mensagem de erro e o backup de dispositivos NAS para conjuntos nativos do IBM Spectrum Protect não será possível. Para evitar conflitos com outros aplicativos, é possível controlar qual porta é adquirida para uso como a porta de dados durante operações de backup de NDMP configurando as opções do servidor NDMPPORTRANGELOW e NDMPPORTRANGEHIGH. Uma porta de dados não é necessária pelo servidor IBM Spectrum Protect porque o NAS restaura a partir dos conjuntos ativos do IBM Spectrum Protect.

### **Problemas de firewall com backup e restauração do servidor NDMP filer-to-IBM Spectrum Protect**

Um firewall pode impedir que o servidor de arquivo de armazenamento conectado à rede (NAS) entre em contato com o servidor IBM Spectrum Protect na porta de dados adquirida durante operações de backup do NAS para um conjunto de armazenamento nativo. Se você tiver que modificar a porta de dados selecionada pelo servidor IBM Spectrum Protect, use as opções do servidor NDMPPORTRANGELOW e NDMPPORTRANGEHIGH.

Um firewall pode impedir que o servidor IBM Spectrum Protect entre em contato com o servidor de arquivos NAS na porta de dados configurada durante operações de restauração do NAS a partir de um conjunto de armazenamentos nativo. Se um firewall impedir que o IBM Spectrum Protect acesse o servidor de arquivos NAS, a conexão de saída do IBM Spectrum Protect falhará.

---

## **Resolvendo Problemas do Dispositivo SCSI**

As unidades e bibliotecas de fita poderão relatar informações novamente para o IBM Spectrum Protect sobre o erro encontrado. Estas informações são relatadas em uma ou mais das mensagens.

Se mensagens ANR8300, ANR8301, ANR8302, ANR8303, ANR8943 ou ANR98944 forem emitidas, os dados que o IBM Spectrum Protect relata a partir desses dispositivos poderão ajudar a determinar as etapas que são necessárias para resolver o problema. Geralmente, quando o servidor relata dados de dispositivo usando essas mensagens, o problema geralmente é com o dispositivo, com a conexão com o dispositivo ou com algum outro problema relacionado fora do IBM Spectrum Protect.

Usando as informações relatadas na mensagem ANR8300, ANR8301, ANR8302, ANR8303, ANR8943 ou ANR98944 do IBM Spectrum Protect, consulte as informações do produto do IBM Spectrum Protect Messages em Mensagens, Códigos de Retorno e Códigos de Erro. Este apêndice documenta informações sobre erros padrão que podem ser relatados por qualquer dispositivo SCSI. Também é possível usar estas informações com a documentação oferecida pelo fornecedor para o hardware para ajudar a determinar a causa e resolução do problema.



---

## Resolvendo Erros de Volume de Mídia Sequencial (Fita) por meio das Mensagens ANR0542W ou ANR8778W

Os problemas que ocorrem com volumes de mídia sequencial podem ser revelados através das mensagens de erro ANR0542W e ANR8778W.

### **ANR0542W A recuperação ou restauração falhou para a sessão *sessionNumber* para o nó *nodeName* - mídia de armazenamento inacessível**

A mensagem de erro ANR0542W geralmente está relacionada a um problema com a unidade ou conexão com a unidade que foi selecionada para ler este volume da fita.

Execute as etapas a seguir para verificar se o IBM Spectrum Protect pode acessar esse volume:

- Emita o comando `QUERY LIBVOL libraryName volumeName`.
- Para uma biblioteca 349X, emita o comando `mtlib -l /dev/lmcp0 -qV volumeName`. Geralmente, o dispositivo é `/dev/lmcp0`, mas, se for diferente, substitua o dispositivo de ponto de controle do gerenciador de biblioteca correto.

As etapas a seguir provavelmente resolvem este problema:

1. Se `mtlib` não relatar este volume, parecerá que este volume está fora da biblioteca. Neste caso, coloque o volume de volta na biblioteca.
2. Se o volume não for relatado por `QUERY LIBVOL`, o servidor não reconhecerá este volume na biblioteca. Emita o comando **CHECKIN LIBVOL** para sincronizar o inventário de biblioteca no servidor com os volumes que estão de fato na biblioteca de fitas.
3. Se os dois comandos relatarem este volume com êxito, provavelmente, a causa será um erro de hardware permanente ou intermitente. Pode haver um erro com a própria unidade ou um erro com a conexão com a unidade. Em qualquer caso, revise os logs de erro de sistema e entre em contato com o fornecedor do hardware para resolver o problema.

### **ANR8778W Volume Utilizável Alterado para Status Privado para Impedir Novo Acesso**

Revise as mensagens do log de atividades para determinar a causa do problema que envolve este volume utilizável. Além disso, revise os logs de erro de sistema e os logs de erros do dispositivo para uma indicação de que ocorreu um problema com a unidade usada para tentar gravar neste volume utilizável.

Se este erro foi causado por uma unidade que requer limpeza ou por algum outro problema específico do hardware que foi resolvido, os volumes que foram configurados para status privado como resultado disto podem ser reconfigurados para utilizáveis emitindo o comando `AUDIT LIBRARY libraryName`.



---

## Apêndice A. Obtendo Informações da Pilha de Chamada de um Arquivo Principal

É possível usar o shell de script gt de amostra fornecido aqui para obter a pilha de chamada para cada encadeamento em execução a partir de um arquivo principal.

Os parâmetros de entrada são o caminho/nome do arquivo executável (./dsmserv padrão) e o caminho/nome do arquivo principal (./dsmcore padrão). O arquivo de saída é dsm\_gdb.info.

**Restrição:** Os arquivos denominados dsm\_gdb.cmd e dsm\_gdb.info são sobrescritos quando esse script é executado.

```
#!/bin/ksh
#
# Se encontrar o seguinte erro:
# ./dsm_gdb.cmd:9: Error in source command file:
# No symbol table is loaded. Use the "file" command.
# then comment out the line that prints buildStringP
#
# if you see other errors, you're on your own ...
exe=${1:-"./dsmserv"} # get parm 1 (executable file path/name), set default
core=${2:-"./dsmcore"} # get parm 2 (core file path/name), set default
echo " "
# look for the executable file ... quit if not found
if [[ -f $exe ]]; then
echo "using executable file:" $exe
else
echo "didn't find executable file ("$exe") ... exiting"
exit
fi
# look for the core file, if not found, look for ./core ... quit if not found
if [[ -f $core ]]; then
echo "using core file:" $core
else
if [[ -f ./core ]]; then
echo "didn't find core file ("$core") but found ./core ... renaming to" $core
mv ./core $core
echo "using core file:" $core
else
echo "didn't find core file ("$core") ... exiting"
exit
fi
fi
echo " "
# make gdb command file to get thread info
nl="\0134\0156" # octal codes for \n (so echo won't think it's \n)
echo "# dsm gdb command file" >|dsm_gdb.cmd
echo "define doit" >>dsm_gdb.cmd
echo "info registers" >>dsm_gdb.cmd # show register values
echo "echo" $nl >>dsm_gdb.cmd
echo "where" >>dsm_gdb.cmd # show function traceback
echo "echo" $nl"===== "$nl >>dsm_gdb.cmd
echo "end" >>dsm_gdb.cmd
echo "echo" $nl"===== "$nl$nl >>dsm_gdb.cmd
echo "x/s buildStringP" >>dsm_gdb.cmd
echo "echo" $nl"===== "$nl$nl >>dsm_gdb.cmd
echo "info threads" >>dsm_gdb.cmd # show thread info
echo "echo" $nl"===== "$nl >>dsm_gdb.cmd
echo "thread apply all doit" >>dsm_gdb.cmd
echo "quit" >>dsm_gdb.cmd
```

```
echo "invoking gdb to get thread info (watch for errors) ..."
echo "if you see:"
echo ". warning: The shared libraries were not privately mapped; setting a"
echo ". breakpoint in a shared library will not work until you rerun the program"
echo "that's ok."
echo "if you see:"
echo ". ./dsm_gdb.cmd:x: Error in source command file:"
echo "then type 'quit', edit this script, and read the comments at the top"
gdb -se $exe -c $core -x ./dsm_gdb.cmd >|dsm_gdb.info
rm dsm_gdb.cmd # done with this now
exit
```

---

## Apêndice B. Executando o Utilitário tsmdiag

É possível diagnosticar problemas com um servidor IBM Spectrum Protect executando o utilitário tsmdiag no sistema em que o servidor IBM Spectrum Protect está instalado. Após coletar os dados diagnósticos, é possível enviar as informações para o Suporte de Software IBM.

### Procedimento

Para executar o utilitário tsmdiag, conclua as seguintes etapas:

1. AIX Linux Altere as permissões do diretório tsmdiag emitindo o seguinte comando:  

```
chmod -R 757 /opt/tivoli/tsm/server/bin/tsmdiag
```
2. Emita o comando **tsmdiag** a partir do seguinte diretório:
  - AIX Linux Usando um ID do usuário da instância do DB2, deve-se emitir o comando **tsmdiag** a partir do diretório /opt/tivoli/tsm/server/bin/tsmdiag.
  - Windows Usando um ID do usuário administrador, deve-se emitir o comando **tsmdiag** a partir do diretório \server\tsmdiag.

Por exemplo, o comando a seguir coleta um conjunto padrão de arquivos de informações de diagnóstico de um servidor IBM Spectrum Protect em um host local. Esse comando é executado por um administrador que é chamado admin com uma senha do administrador admin01 em um servidor IBM Spectrum Protect. Este servidor está em execução na porta TCP/IP 1501 de um host local.

```
tsmdiag -id admin -pa admin01 -tcpport 1501
```

3. Obtenha o arquivo de resultados do seguinte diretório:
  - AIX Linux /opt/tivoli/tsm/server/bin/tsmdiag/results/tsmdiag\_results<year>-<month>-<day>-<hour>-<minute>-<second>.tar
  - Windows C:\Program Files\tivoli\tsm\server\tsmdiag\results\tsmdiag\_results<year>-<month>-<day>-<hour>-<minute>-<second>.zip
4. Envie o arquivo de resultados com o relatório de problemas para o Suporte de Software IBM.

### Comandos tsmdiag de exemplo

O comando a seguir conecta-se a um servidor IBM Spectrum Protect chamado MYSERVER na porta TCP/IP 1501. Quando um administrador DB2 chamado admin executa o seguinte comando, um conjunto padrão de arquivos de informações de diagnóstico é coletado. As informações de diagnóstico sobre o desempenho do servidor MYSERVER também são coletadas.

```
tsmdiag -id admin -pa admin01 -tcpport 1501 -servername MYSERVER -performance
```

O comando a seguir conecta-se a um servidor IBM Spectrum Protect na porta TCP/IP padrão 1500. Quando um administrador chamado admin executar o seguinte comando, o comando coletará um conjunto padrão de arquivos de informações de diagnóstico. Este comando também fornece resultados dos comandos **SHOW** do servidor IBM Spectrum Protect e algumas informações de diagnóstico sobre o status do servidor IBM Spectrum Protect.

## Opções do utilitário tsmddiag

Use o utilitário tsmddiag para ajudar a diagnosticar problemas com um componente do servidor IBM Spectrum Protect. Ao executar o utilitário, é possível especificar opções que determinam o tipo de informações de diagnóstico fornecidas.

É possível especificar as seguintes opções ao emitir o comando **tsmddiag**:

**id adminName**

O ID de administrador ou usuário root do servidor no qual executar o comando **tsmddiag**. Esta opção é obrigatória.

**-pa adminPwd**

A senha do ID do administrador ou do usuário root. Esta opção é obrigatória.

**-tcpserveraddress ipAddress**

Especifica o nome ou endereço TCP/IP do servidor no qual executar o comando **tsmddiag**. A opção é opcional. O valor padrão é localhost.

**-tcpport portNumber**

Especifica a porta TCP/IP do servidor no qual executar o comando **tsmddiag**. Esta opção é opcional. O valor padrão é 1500.

AIX

Linux

**-servername**

O nome do servidor no qual executar o comando **tsmddiag**. Esta opção é opcional. O valor padrão é SERVER1.

**-crash** Especifica se relatar se o servidor falhou. Esta opção é opcional. O valor padrão é off.

**-dbcorrupt**

Especifica se relatar se existe dano no banco de dados. Esta opção é opcional. O valor padrão é off.

**-dbgrowth**

Especifica se relatar se há aumento excessivo de banco de dados grande no servidor. Esta opção executa o script serverReorgInfo.pl e o script tsmddiag\_dedup\_stats.pl, que produzem informações de diagnóstico adicionais. O script serverReorgInfo.pl demora mais de 1 hora para ser executado. Esta opção é opcional. O valor padrão é off.

**-hang** Especifica se relatar se o servidor está sendo interrompido. Esta opção é opcional. O valor padrão é off.

**-performance**

Especifica se relatar se há problemas de desempenho com o servidor. Esta opção executa o script tsmddiag\_sysmonv6.pl, que produz informações extras de diagnóstico. O script tsmddiag\_sysmonv6.pl pode demorar 1 hora e meia para ser executado. Esta opção é opcional. O valor padrão é off.

**-v** Especifica se a saída de relatório é produzida em formato detalhado. Esta opção é opcional. O valor padrão é off.

**-?** Especifica as informações de uso para o utilitário tsmddiag. Se você emitir o comando tsmddiag ?, uma lista de opções anteriores será exibida.

---

## Apêndice C. Códigos de Retorno do IBM Global Security Kit

O servidor e o cliente usam o processamento IBM Global Security Kit (GSKit) para SSL (Secure Sockets Layer) entre o servidor e o cliente de backup-archive. Algumas mensagens são emitidas para o processamento de SSL incluem códigos de retorno GSKit.

O GSKit é automaticamente instalado ou atualizado durante a instalação do IBM Spectrum Protect e fornece as seguintes bibliotecas:

- SSL GSKit
- API de Gerenciamento de Chaves do GSKit
- IBM Crypto para C (ICC)

O utilitário tsmdiag relata o nível de GSKit que está instalado em seu sistema ou é possível usar um dos seguintes métodos:

- Para Windows, emita os seguintes comandos:  

```
regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\"  
notepad gskitinfo.txt
```

### **CUIDADO:**

**O sistema pode ser danificado se você usar regedit incorretamente.**

- Para o servidor AIX de 64 bits, emita o seguinte comando a partir da linha de comandos: gsk8ver\_64

Consulte a Tabela 17 para obter os códigos de retorno SSL GSKit.

O servidor usa a API de GSKit Key Management para criar automaticamente o banco de dados de gerenciamento de chaves e as chaves pública e privada do servidor. Algumas mensagens emitidas para esse processamento podem incluir códigos de retorno do Gerenciamento de Chave do Global Security Kit. Consulte a Tabela 18 na página 218 para obter os códigos de retorno de gerenciamento de chaves.

*Tabela 17. Códigos de Retorno Gerais do SSL do IBM Global Security Kit*

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x00000000	0	GSK_OK	A tarefa foi concluída com êxito. Emitida por cada chamada de função concluída com êxito.
0x00000001	1	GSK_INVALID_HANDLE	O ambiente ou a manipulação SSL não é válida. O identificador especificado não era o resultado de uma chamada de função open() bem-sucedida.
0x00000002	2	GSK_API_NOT_AVAILABLE	A biblioteca de links dinâmicos (DLL) foi descarregada e não está disponível (ocorre apenas nos sistemas Microsoft Windows).
0x00000003	3	GSK_INTERNAL_ERROR	Erro interno. Reporte esse erro ao IBM Software Support.

Tabela 17. Códigos de Retorno Gerais do SSL do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x00000004	4	GSK_INSUFFICIENT_STORAGE	A memória disponível é insuficiente para concluir a operação.
0x00000005	5	GSK_INVALID_STATE	O identificador não está em um estado válido para operação, como concluindo uma operação <code>init()</code> duas vezes em um identificador.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	O rótulo chave especificado não foi localizado no arquivo-chave.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	O certificado não foi recebido do parceiro.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Erro de validação do certificado.
0x00000009	9	GSK_ERROR_CRYPT0	Erro ao processar criptografia.
0x0000000a	10	GSK_ERROR_ASN	Erro ao validar campos ASN no certificado.
0x0000000b	11	GSK_ERROR_LDAP	Erro ao conectar-se ao registro do usuário.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Erro interno. Reporte esse erro ao IBM Software Support.
0x0000000d	13	GSK_INVALID_PARAMETER	Parâmetro inválido.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Parâmetro inválido. Reporte esse erro ao IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Erro interno. Reporte esse erro ao IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Erro de E/S ao ler o arquivo de chaves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	O arquivo de chaves não possui um formato interno válido. Recriar o arquivo-chave.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	O arquivo de chaves possui duas entradas com a mesma chave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	O arquivo de chaves possui duas entradas com o mesmo rótulo.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	A senha do arquivo de chaves foi usada como uma verificação de integridade. Ou o arquivo-chave está corrompido ou a ID de senha está incorreta.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	A chave padrão no arquivo de chaves possui um certificado expirado.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Ocorreu um erro ao carregar uma das bibliotecas de links dinâmicos do GSK. Verifique se o GSK foi instalado corretamente.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Indica que está ocorrendo uma tentativa de conexão em um ambiente do GSK após a configuração do <code>GSK_ENVIRONMENT_CLOSE_OPTIONS</code> como <code>GSK_DELAYED_ENVIRONMENT_CLOSE</code> e após a chamada da função <code>gsk_environment_close()</code> .



Tabela 17. Códigos de Retorno Gerais do SSL do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	A senha e o nome do arquivo stash não foram especificados. O arquivo-chave não é inicializado.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Não é possível abrir o arquivo de chaves. O caminho foi especificado incorretamente ou as permissões do arquivo não permitiram que o arquivo fosse aberto.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Não é possível gerar um parte de chaves temporárias. Reporte esse erro ao IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Um objeto de nome de usuário especificado não foi localizado.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Uma senha usada por uma consulta de LDAP (protocolo LDAP) não está correta.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Um índice na lista Com Falha de servidores LDAP não estava correto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalação do GSKit não suporta o modo de operação FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que o pedido de fechamento do ambiente do GSK não foi gerenciado corretamente. A causa mais provável é ter ocorrido uma tentativa de comando <code>gsk_secure_socket*()</code> após uma chamada de <code>gsk_close_environment()</code> .
0x00000191	401	GSK_ERROR_BAD_DATE	A data do sistema não foi configurada como um valor válido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	O SSLv2 e o SSLv3 não estão ativos.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	O certificado necessário não foi recebido do parceiro.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	O certificado recebido foi formatado incorretamente.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	O tipo de certificado recebido não era suportado.
0x00000196	406	GSK_ERROR_IO	Ocorreu um erro de E/S em uma operação de leitura ou gravação de dados.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	A etiqueta especificada no arquivo-chave não foi localizada.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	A senha do arquivo de chaves especificada está incorreta. O arquivo-chave não pode ser usado. O arquivo de chaves também pode estar danificado.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	Em um ambiente de criptografia restrito, o tamanho da chave é muito longo para ser suportado.

Tabela 17. Códigos de Retorno Gerais do SSL do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Uma mensagem SSL formatada incorretamente foi recebida do parceiro.
0x0000019b	411	GSK_ERROR_BAD_MAC	O message authentication code (MAC) não foi verificado com êxito.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL não suportado ou tipo de certificado não suportado.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	O certificado recebido continha uma assinatura incorreta.
0x0000019e	414	GSK_ERROR_BAD_CERT	O certificado formatado incorretamente foi recebido do parceiro.
0x0000019f	415	GSK_ERROR_BAD_PEER	Não recebeu um protocolo SSL válido do parceiro.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Reporte esse erro ao IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	O certificado autoassinado não é válido.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	Falha de read(). Reporte esse erro ao IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	Falha de write(). Reporte esse erro ao IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	O parceiro fechou o soquete antes da conclusão do protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	O código V2 especificado não é válido.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	O código V3 especificado não é válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Reporte esse erro ao IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Reporte esse erro ao IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	O identificador não pode ser criado. Reporte esse erro ao IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Ocorreu uma falha na inicialização. Relate este erro interno para o serviço.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Não foi possível acessar o registro do usuário especificado quando um certificado está sendo validado.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	A chave especificada não continha uma chave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Foi feita uma tentativa falha de carregar a biblioteca compartilhada PKCS11 especificada.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	O driver PKCS #11 falhou ao localizar o token especificado pelo responsável pela chamada.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	Um token PKCS #11 não está presente no slot.

Tabela 17. Códigos de Retorno Gerais do SSL do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	A senha/pin para acessar o token PKCS #11 não é válida.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	O cabeçalho SSL recebido não era um cabeçalho SSLv2 formatado corretamente.
0x000001b2	434	GSK_CSP_OPEN_ERROR	Não é possível abrir o provedor de serviços criptográficos com base no hardware. O nome de CSP não está especificado corretamente ou foi feita uma tentativa com falha de acessar o armazenamento de certificados CSP especificado.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Conflito de configuração de atributo entre PKCS11, o banco de dados de chaves CMS e a API Microsoft Crypto.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	A função solicitada não é suportada na plataforma na qual o aplicativo está executando. Por exemplo, a API Microsoft Crypto não é suportada nas plataformas diferentes de Windows 2000.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Valor incorreto é retornado da função de retorno de chamada de tipo de sessão redefinida. Apenas GSKit gsk_sever_session, gsk_sever_session_with_cl_auth ou gsk_sever_session_with_cl_auth_crit é permitido.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	O tamanho do buffer é negativo ou zero.
0x000001f6	502	GSK_WOULD_BLOCK	Usado com E/S nonblocking. Consulte a seção nonblocking para uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 é necessário para reset_cipher(), e a conexão usa SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Não foi especificado um ID válido para a chamada de função gsk_secure_soc_misc().
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	A chamada de função não possui um ID válido. Esse problema também pode ser causado especificando um manipulador de ambiente quando um identificador para uma conexão SSL deveria ser usado.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	O atributo possui um comprimento negativo, que não é válido.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	O valor de enumeração não é válido para o tipo de enumeração especificado.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	A lista de parâmetros não é válida para substituir as rotinas de cache SID.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Quando um atributo numérico é configurado, o valor especificado não é válido para o atributo específico que está sendo configurado.

Tabela 17. Códigos de Retorno Gerais do SSL do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Parâmetros em conflito foram configurados para validação adicional de certificado.
0x000002c3	707	GSK_AES_UNSUPPORTED	O algoritmo criptográfico AES não é suportado.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	O PEERID não possui o comprimento correto.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	A cifra particular não é permitida quando o modo de operação FIPS estiver desativado.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	Nenhuma cifra FIPS aprovada é selecionada no modo de operação FIPS.
0x00000641	1601	GSK_TRACE_STARTED	O rastreo foi iniciado com êxito.
0x00000642	1602	GSK_TRACE_STOPPED	O rastreo foi interrompido com êxito.
0x00000643	1603	GSK_TRACE_NOT_STARTED	Nenhum arquivo de rastreo foi iniciado anteriormente, portanto, ele não pode ser interrompido.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	O arquivo de rastreo é iniciado, portanto, não pode ser reiniciado.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	O arquivo de rastreo não pode ser aberto. O primeiro parâmetro de gsk_start_trace() deve ser um nome do arquivo de caminho completo válido.

Tabela 18. Códigos de Retorno de Gerenciamento de Chaves do IBM Global Security Kit

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x00000000	0	GSK_OK	A tarefa foi concluída com êxito. Essa mensagem é emitida por cada chamada de função concluída com êxito.
0x00000001	1	GSK_INVALID_HANDLE	O ambiente ou a manipulação SSL não é válida. O identificador especificado não era o resultado de uma chamada de função open() bem-sucedida.
0x00000002	2	GSK_API_NOT_AVAILABLE	A DLL (biblioteca de links dinâmicos) foi descarregada e não está disponível (ocorre apenas nos sistemas Microsoft Windows).
0x00000003	3	GSK_INTERNAL_ERROR	Erro interno. Reporte esse erro ao IBM Software Support.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	A memória disponível é insuficiente para concluir a operação.

Tabela 18. Códigos de Retorno de Gerenciamento de Chaves do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x00000005	5	GSK_INVALID_STATE	O identificador está em um estado incorreto para operação, como concluindo uma operação init() duas vezes em um identificador.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	O rótulo chave especificado não foi localizado no arquivo-chave.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	O certificado não foi recebido do parceiro.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Erro de validação do certificado.
0x00000009	9	GSK_ERROR_CRYPTO	Erro ao processar criptografia.
0x0000000a	10	GSK_ERROR_ASN	Erro ao validar campos ASN no certificado.
0x0000000b	11	GSK_ERROR_LDAP	Erro ao conectar-se ao registro do usuário.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Erro interno. Reporte esse erro ao IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Erro interno. Reporte esse erro ao IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Erro de E/S ao ler o arquivo de chaves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	O arquivo de chaves possui um formato interno inválido. Recrie o arquivo de chaves.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	O arquivo de chaves possui duas entradas com a mesma chave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	O arquivo de chaves possui duas entradas com o mesmo rótulo.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	A senha do arquivo de chaves foi usada como uma verificação de integridade. Ou o arquivo-chave está corrompido ou a ID de senha está incorreta.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	A chave padrão no arquivo de chaves possui um certificado expirado.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Ocorreu um erro enquanto uma das bibliotecas de link dinâmico era carregada. Verifique se o GSK foi instalado corretamente.

Tabela 18. Códigos de Retorno de Gerenciamento de Chaves do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Esta mensagem indica que uma conexão está tentando ser feita em um ambiente do GSK depois que GSK_ENVIRONMENT_CLOSE_OPTIONS foi configurado para GSK_DELAYED_ENVIRONMENT_CLOSE e a função gsk_environment_close() foi chamada.
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	A senha e o nome do arquivo stash não foram especificados, portanto, o arquivo-chave não é inicializado.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Não é possível abrir o arquivo de chaves. O caminho foi especificado incorretamente ou as permissões do arquivo não permitiram que o arquivo fosse aberto.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Não é possível gerar um parte de chaves temporárias. Reporte esse erro ao IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Um objeto de nome de usuário especificado não foi localizado.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Uma senha usada para uma consulta de LDAP não está correta.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Um índice na lista Com Falha de servidores LDAP não estava correto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalação do GSKit não suporta o modo de operação FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que o pedido de fechamento do ambiente do GSK não foi gerenciado corretamente. A causa mais provável é que houve tentativa de um comando gsk_secure_socket*() após uma chamada gsk_close_environment().
0x00000191	401	GSK_ERROR_BAD_DATE	A data do sistema foi configurada como um valor inválido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	SSLv2 e SSLv3 não estão ativos.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	O certificado necessário não foi recebido do parceiro.

Tabela 18. Códigos de Retorno de Gerenciamento de Chaves do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	O certificado recebido foi formatado incorretamente.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	O tipo de certificado recebido não era suportado.
0x00000196	406	GSK_ERROR_IO	Ocorreu um erro de E/S em uma operação de leitura ou gravação de dados.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	A etiqueta especificada no arquivo-chave não foi localizada.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	A senha do arquivo de chaves especificada está incorreta. O arquivo-chave não pode ser usado. O arquivo-chave também pode estar corrompido.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_ FOR_EXPORT	Em um ambiente de criptografia restrito, o tamanho da chave é muito longo para ser suportado.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Uma mensagem SSL formatada incorretamente foi recebida do parceiro.
0x0000019b	411	GSK_ERROR_BAD_MAC	O MAC não foi verificado com êxito.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL não suportado ou tipo de certificado não suportado.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	O certificado recebido continha uma assinatura incorreta.
0x0000019e	414	GSK_ERROR_BAD_CERT	O certificado formatado incorretamente foi recebido do parceiro.
0x0000019f	415	GSK_ERROR_BAD_PEER	Um protocolo SSL não válido é recebido do parceiro.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Reporte esse erro ao IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	O certificado autoassinado não é válido.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	Falha de read(). Reporte esse erro ao IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	Falha de write(). Reporte esse erro ao IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	O parceiro fechou o soquete antes da conclusão do protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	O código V2 especificado não é válido.

Tabela 18. Códigos de Retorno de Gerenciamento de Chaves do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	O código V3 especificado não é válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Reporte esse erro ao IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Reporte esse erro ao IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	O identificador não é criado. Reporte esse erro ao IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Ocorreu uma falha na inicialização. Relate este erro interno para o serviço.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Não é possível acessar o registro do usuário especificado quando um certificado está sendo validado
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	A chave especificada não continha uma chave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Foi feita uma tentativa falha de carregar a biblioteca compartilhada PKCS11 especificada.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	O driver PKCS #11 falhou ao localizar o token especificado pelo responsável pela chamada.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	Um token PKCS #11 não está presente no slot.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	A senha/pin para acessar o token PKCS #11 está incorreta.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	O cabeçalho SSL recebido não era um cabeçalho SSLv2 formatado corretamente.
0x000001b2	434	GSK_CSP_OPEN_ERROR	Não foi possível abrir o provedor de serviço criptográfico baseado em hardware (CSP). O nome de CSP não está especificado corretamente ou foi feita uma tentativa com falha de acessar o armazenamento de certificados CSP especificado.
0x000001b3	435	GSK_CSP_OPEN_ERROR	Foram definidos alguns atributos conflitantes para a operação de SSL.
0x000001b4	436	GSK_CSP_OPEN_ERROR	A API Microsoft Crypto é suportada apenas no Microsoft Windows 2000 com Service Pack 2 aplicado.



Tabela 18. Códigos de Retorno de Gerenciamento de Chaves do IBM Global Security Kit (continuação)

Código de Retorno (hex)	Código de Retorno (decimal)	Constante	Explicação
0x000001b5	437	GSK_CSP_OPEN_ERROR	O sistema está em execução no modo IPv6 sem configurar um PEERID.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	O tamanho do buffer é negativo ou zero.
0x000001f6	502	GSK_WOULD_BLOCK	Usado com E/S nonblocking. Consulte a seção nonblocking para uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 é necessário para <code>reset_cipher()</code> , e a conexão usa SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Foi especificado um ID inválido para a chamada de função <code>gsk_secure_soc_misc()</code> .
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	A chamada de função possui um ID inválido. Esse problema também pode ser causado especificando um manipulador de ambiente quando um identificador para uma conexão SSL deveria ser usado.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	O atributo possui um comprimento negativo, que não é válido.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	O valor de enumeração não é válido para o tipo de enumeração especificado.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	A lista de parâmetros não é válida para substituir as rotinas de cache SID.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Quando um atributo numérico é configurado, o valor especificado não é válido para o atributo específico que está sendo configurado.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Parâmetros em conflito foram configurados para validação adicional de certificado.
0x000002c3	707	GSK_AES_UNSUPPORTED	O algoritmo criptográfico AES não é suportado.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	O PEERID não possui o comprimento correto.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	A cifra particular não é permitida quando o modo de operação FIPS estiver desativado.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	Nenhuma cifra FIPS aprovada é selecionada no modo de operação FIPS.

*Tabela 18. Códigos de Retorno de Gerenciamento de Chaves do IBM Global Security Kit (continuação)*

<b>Código de Retorno (hex)</b>	<b>Código de Retorno (decimal)</b>	<b>Constante</b>	<b>Explicação</b>
0x00000641	1601	GSK_TRACE_STARTED	O rastreo foi iniciado com êxito.
0x00000642	1602	GSK_TRACE_STOPPED	O rastreo foi interrompido com êxito.
0x00000643	1603	GSK_TRACE_NOT_STARTED	Nenhum arquivo de rastreo foi iniciado anteriormente, portanto, ele não pode ser interrompido.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	O arquivo de rastreo é iniciado, portanto, não pode ser iniciado novamente.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	O arquivo de rastreo não pode ser aberto. O primeiro parâmetro de gsk_start_trace() deve ser um nome de arquivo válido, com caminho completo.

---

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

Os recursos de acessibilidade ajudam usuários com deficiência, como mobilidade restrita ou visão limitada, a usarem o conteúdo da tecnologia da informação com sucesso.

### Visão geral

A família de produtos IBM Spectrum Protect inclui os seguintes recursos principais de acessibilidade:

- Operação apenas do teclado
- Operações que usam um leitor de tela

A família de produtos IBM Spectrum Protect usa o W3C Standard mais recente, WAI-ARIA 1.0 ([www.w3.org/TR/wai-aria/](http://www.w3.org/TR/wai-aria/)), para assegurar conformidade com o US Section 508 ([www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards)) e Web Content Accessibility Guidelines (WCAG) 2.0 ([www.w3.org/TR/WCAG20/](http://www.w3.org/TR/WCAG20/)). Para aproveitar os recursos de acessibilidade, use a liberação mais recente do seu leitor de tela e o navegador da web mais recente que seja suportado pelo produto.

A documentação do produto no IBM Knowledge Center está ativada para acessibilidade. Os recursos de acessibilidade do IBM Knowledge Center são descritos na Seção Acessibilidade da Ajuda do IBM Knowledge Center ([www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility](http://www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility)).

### Navegação pelo teclado

Este produto usa teclas de navegação padrão.

### Informações de interface

As interfaces com o usuário não têm conteúdo que atualiza de 2 a 55 vezes por segundo.

As interfaces com o usuário da web dependem das folhas de estilo em cascata para renderizar o conteúdo adequadamente e para fornecer uma experiência utilizável. O aplicativo fornece uma maneira equivalente para usuários com pouca visão para usarem configurações de exibição do sistema, incluindo o modo de alto contraste. É possível controlar o tamanho da fonte usando o dispositivo ou as configurações 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 IBM Spectrum Protect inclui certos softwares do fornecedor que não são cobertos 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 TTY  
800-IBM-3383 (800-426-3383)  
(na América do Norte)

Para obter mais informações sobre o compromisso que a IBM tem com a acessibilidade, consulte Acessibilidade IBM([www.ibm.com/able](http://www.ibm.com/able)).

---

## Avisos

Estas informações foram elaboradas para produtos e serviços oferecidos nos EUA. Este material pode estar disponível na IBM em outros idiomas. No entanto, pode ser necessário ter uma cópia do produto ou da versão de produto nesse idioma para acessá-lo.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos neste documento em outros países. Consulte seu representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a um produto, programa ou serviço IBM não significa que somente esse produto, programa ou serviço IBM possa 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 descritos neste documento. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

*Gerência de Relações Comerciais e Industriais da IBM Brasil*  
*Av. Pasteur, 138-146*  
*Botafogo*  
*Rio de Janeiro, RJ*  
*CEP 22290-240*

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

*Intellectual Property Licensing*  
*Legal and Intellectual Property Law*  
*IBM Japan Ltd.*  
*19-21, Nihonbashi-Hakozakicho, Chuo-ku*  
*Tokyo 103-8510, Japan*

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO-INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, 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) a utilização mútua das informações trocadas, devem entrar em contato com:

*Gerência de Relações Comerciais e Industriais da IBM Brasil*  
*Av. Pasteur, 138-146*  
*Botafogo*  
*Rio de Janeiro, RJ*  
*CEP 22290-240*

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito nesta publicação e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato Internacional de Licença do Programa IBM ou de qualquer outro contrato equivalente.

Os dados de desempenho discutidos aqui são apresentados como derivados de condições operacionais 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 publicamente disponíveis. A IBM não testou estes produtos e não pode confirmar a precisão do desempenho, compatibilidade ou qualquer outra reivindicação relacionada a produtos não-IBM. Perguntas sobre os recursos de produtos não IBM devem ser encaminhadas diretamente 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, uso, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas de amostra são fornecidos

"NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não deve ser responsabilizado por quaisquer danos oriundos do uso dos programas de amostra.

Qualquer cópia, parte desses programas de amostra ou trabalho derivado deve incluir um aviso de copyright da seguinte forma: © (o nome de sua empresa) (ano). Partes deste código são derivadas dos Programas de Amostras da IBM Corp. © Copyright IBM Corp. \_digite o(s) ano(s)\_.

## **Marcas comerciais**

IBM, o logotipo IBM e [ibm.com](http://ibm.com) são marcas comerciais ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas comerciais da IBM ou de outras empresas. Uma lista atual de marcas comerciais da IBM está disponível na web em "Copyright and trademark information" em [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe é uma marca registrada da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Linear Tape-Open, LTO e Ultrium são marcas comerciais da HP, IBM Corp. e Quantum nos Estados Unidos e em outros países.

Intel e Itanium são marcas comerciais ou marcas registradas da Intel Corporation ou de suas subsidiárias nos Estados Unidos e em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows e Windows NT são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas da Oracle e/ou suas afiliadas.

SoftLayer é uma marca registrada da SoftLayer, Inc., uma empresa IBM.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

## **Termos e condições para a documentação do produto**

As permissões para o uso dessas publicações são concedidas, sujeitas aos seguintes termos e condições.

### **Aplicabilidade**

Esses termos e condições são adicionais a quaisquer termos de uso para o website da IBM.

### **Uso Pessoal**

É possível reproduzir estas publicações para seu uso pessoal, não comercial, desde que todos os avisos do proprietário sejam preservados. Você não pode distribuir, exibir ou realizar trabalho derivado dessas publicações, ou de qualquer parte delas, sem consentimento expresso da IBM.

### **Uso Comercial**

É possível reproduzir, distribuir e exibir essas publicações somente dentro da empresa, desde que todos os avisos do proprietário sejam preservados. Não é permitido realizar trabalhos derivados dessas publicações nem reproduzir, distribuir ou exibir essas publicações ou qualquer parte delas fora da 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 o direito de retirar as permissões aqui concedidas sempre que, por decisão própria, o uso das publicações for prejudicial a seu interesse, conforme determinado pela IBM, as instruções acima não forem seguidas corretamente.

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 da política de privacidade**

Os produtos de Software IBM, incluindo o software como soluções de serviços, ("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 ajudar a permitir a coleta de informações de identificação pessoal. Se esta Oferta de software usar cookies para coletar informações de identificação pessoal, informações específicas sobre o uso de cookies dessa oferta são determinadas abaixo.

Esta Oferta de software não usa cookies ou outras tecnologias para coletar informações de identificação pessoal.

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 mais informações sobre o uso de várias tecnologias para esses propósitos, incluindo cookies, consulte a Política de privacidade da IBM em <http://www.ibm.com/privacy> e a Declaração de privacidade da IBM em <http://www.ibm.com/privacy/details> na seção intitulada "Cookies, Web Beacons e Outras Tecnologias," e "IBM Software Products and Software-as-a-Service Privacy Statement" em <http://www.ibm.com/software/info/product-privacy>.



---

## **Glossário**

Está disponível um glossário com termos e definições para a família de produtos IBM Spectrum Protect.

Consulte o IBM Spectrum Protectglossário.

Para visualizar glossários para outros produtos IBM, consulte IBM Terminology.



---

# Índice Remissivo

## A

- administradores
  - bloqueados 14
- agente de armazenamento
  - configuração sem LAN
    - conjunto de armazenamentos configurado para gravação simultânea 118
    - dados enviados diretamente para o servidor 116
    - testando a configuração sem LAN 118
  - dicas de diagnóstico
    - erro causado por leitura ou gravação em um dispositivo 115
    - problemas causados pela mudança nas opções do servidor 116
    - problemas de mudança de opções do agente de armazenamento 116
    - verificar o log de atividades do servidor 115
  - dispositivos SAN 195
- agentes de monitoramento
  - ativando o rastreo 172, 174
- AIX JFS2
  - backup-archive baseado em captura instantânea 33
  - backup de imagem 33
- ajuda
  - servidor ou agente de armazenamento 2
- ajuste da Microsoft VSS 46
- alertas
  - atraso no fechamento ou designação 107
- alocando memória adicional 59
- ANR1221E
  - mensagem de erro 93
- ANR2317W
  - mensagem de erro 94
- API
  - arquivo de opções 37
- aplicativo de backup
  - arquivos automaticamente excluídos 22
  - arquivos excluídos devido à frequência de cópia incremental 61
  - arquivos excluídos por EXCLUDE DIR 24
  - arquivos excluídos por instruções de inclusão/exclusão 21
  - inclusão/exclusão devido a instruções de compactação, criptografia e backup de subarquivo 26
  - instruções de inclusão/exclusão codificadas incorretamente 27
  - instruções de inclusão/exclusão específicas da plataforma 26
- arquivo de banco de dados de chaves
  - fora de sincronização 112
  - recuperação de senha 112
- arquivo de configuração de criação de log 120
- arquivo de ID do banco de dados ausente ou incorreto 80
- arquivos de log 105, 106, 119, 120
  - instalação 64
  - upgrade do DB2 80
- arquivos de log do DB2 79
- autenticação de senha
  - configuração do cliente 11
- autoridade de certificação 110

## B

- backup baseado em diário (JBB)
  - determinando 42
  - executando em primeiro plano 43
  - utilitário de visualização do banco de dados 43
- BACKUP DB
  - ANR2971E com o código SQL 83
  - erros comuns 85
  - variáveis de ambiente incorretas 82
- backup de imagem
  - cliente 31
  - erro 31, 32

## C

- cache
  - ignorar durante operações de gravação 186
- cancelar diversas tarefas
  - atraso 107
- Centro de Operações
  - problemas conhecidos 108
- classes de rastreo
  - cliente 154
  - servidor ou agente de armazenamento 124
- cliente
  - backup de imagem 31
  - classes de rastreo 154, 160
  - falha de autenticação 10
  - gerando erros
    - conectado ao servidor 109
  - identificando quando e onde os problemas ocorrem 5
  - log de atividades do servidor
    - examinando 5
  - mensagens de erro
    - examinando 5
  - o problema pode ser reproduzido 6
  - resolvendo problemas 5
  - scheduler 18
- cliente de backup-archive
  - ajuda 1
  - comandos SHOW 48
- comando DELETE KEYRING 113
- comando IMPORT 62
- comando SET LDAPPASSWORD
  - problemas relacionados a 12
- comandos administrativos
  - DELETE KEYRING 113
- comandos SHOW
  - servidor ou agente de armazenamento 140
- configuração sem LAN
  - agente de armazenamento 116
- conjuntos de opções do cliente
  - resolvendo problemas 9
  - utilização 9

## D

- dados
  - enviados para o agente de armazenamento ou o servidor 38

- dados (*continuação*)
  - ilegíveis 177
- dados compactados durante o backup-archive 170
- dados criptografados durante o backup-archive 170
- dados de rastreo
  - são compactados durante o backup-archive 170
  - são criptografados durante o backup-archive 170
- designar diversos alertas
  - atraso 107
- diário
  - reiniciando 43
- dicas de diagnóstico
  - agente de armazenamento 115
  - cliente 5
- dicas e sugestões
  - configuração da SAN 191
  - driver de dispositivo 180
  - mapeamento de dispositivos SAN 197
  - Operações do arquivador NDMP para o servidor IBM Spectrum Protect 205
  - SAN 190
  - subsistemas de disco 185
  - unidades de disco rígido 185
  - unidades e bibliotecas de fitas
    - adaptador substituído 189
    - conexões com cabo solto 190
    - mensagens de erro no log de erro de sistema 190
    - mudanças no cabeamento entre o computador e o dispositivo 188
    - mudanças no driver de dispositivo 189
    - mudanças no firmware do adaptador 188
    - mudanças no firmware do dispositivo 188
    - mudanças no sistema operacional 189
    - outro hardware alterado ou corrigido 189
- Diferença de Captura Instantânea
  - resolvendo problemas 27
- diretório db2dump
  - resolução de encerramento 73
- diretório de captura instantânea 30
- dispositivos SAN
  - agente de armazenamento 195
- dispositivos SCSI 206
- documentação
  - para resolver problemas do cliente 6
- driver de dispositivo
  - atualizando informações sobre o dispositivo 184
  - conexão com cabo solto 181
  - drivers HBA em kernels Linux 2.6.x 183
  - executando ddtrace a partir da versão 5.3.2 no Linux 184
  - mensagens de erro no log de erro de sistema 182
  - módulos de kernel Linux de 32 bits 182
  - módulos de kernel Linux de 64 bits 182
  - mudanças no adaptador SCSI 181
  - mudanças no HBA 181
  - mudanças no sistema operacional 181
  - requisitos de Adaptec SCSI 185
  - requisitos de BIOS HBA Qlogic fibre-channel 185
  - servidor Linux em execução na arquitetura x86\_64 182
  - suporte a vários LUNs em kernels Linux 183
- dmsanlist 192, 197, 201, 205

## E

- erro de backup de imagem da Captura Instantânea do Linux
  - mensagem de erro ANS1258E 32
- erro de backup de imagem do Linux 31

- erros de comunicação
  - resolvendo 109
- erros de restauração do banco de dados 80
- erros temporários
  - VSS 45
- Evento Planejado
  - status 18

## F

- falha de verificação de página do banco de dados 75
- fechar diversos alertas
  - atraso 107
- frequência de cópia 61

## G

- gerenciador do banco de dados
  - problemas de inicialização 75
- grupos de criação de log 119, 120
- GSKit
  - códigos de retorno 213
  - problemas de instalação 65

## I

- IBM Global Security Kit
  - códigos de retorno 213
  - códigos de retorno de gerenciamento de chaves 213
- IBM Knowledge Center vii
- ID do Usuário \$\$\_TSMDBMGR\_\$\$ Oculto 86
- ID do usuário não raiz
  - executando aplicativos usando a API 39
- implementação automática
  - resolução de problemas 67
- implementação do cliente
  - resolução de problemas 67
- incapacidade 225
- informações de diagnóstico da Microsoft
  - VSS 47
- Installation Manager
  - diretório de logs 64
- instância do servidor
  - configurando 60
- Interface de Programação de Aplicativos (API)
  - instrumentação 35
  - rastreamento 171
- interrupção do servidor
  - arquivo de erros do servidor (dmserv.err) 70
  - arquivos de biblioteca 72
  - imagem do sistema 71
  - log de atividades 73
  - logs do sistema 72
  - resolvendo problemas gerais 68
- interrupção na desinstalação 67

## K

- Knowledge Center vii

## L

- LABEL LIBVOLUME 61
- limitações
  - do Centro de Operações 108

limite de memória 78  
log de atividades do servidor  
verificando erros 19  
log de planejamento de cliente 19

## M

mapeamento de diretório FILE 187  
mapeamento de dispositivos SAN  
ausente da exibição de QUERY SAN 203  
desativando 198  
erros 198  
memória compartilhada 60  
Memória do DB2 78  
mensagens de erro  
ANR1330E 95  
ANR1331E 95  
ANR2968E 83  
senhas autenticadas por LDAP 15  
mensagens de erro do banco de dados 81  
movendo dados para outros volumes 187

## N

nós  
bloqueados 14  
nós e administradores bloqueados 14  
ntbackup.exe 48

## O

opção INCLEXCL 21  
opções 212  
Operations Center  
resolução de problemas 105, 106, 119  
solução de problemas 105, 119, 120

## P

problemas conhecidos  
com o Centro de Operações 108  
problemas de inicialização  
dsm 7  
dsmadm 7  
dsmc 7  
dsmj 7  
problemas de instalação 64  
problemas de upgrade 64  
processo iniciado 91  
processo terminado 91  
processos  
atraso no cancelamento 107  
programa de amostra vsreq.exe 48  
programas  
dsm 7  
dsmadm 7  
dsmc 7  
dsmj 7  
publicações vii

## R

rastreando 106, 119, 120  
agentes 172, 174  
cliente 152

rastreando (*continuação*)

Interface de Programação de Aplicativos (API) 171  
Plug-in de ID de Usuário/Senha 77

rastreio

ativar rastreio do cliente enquanto o cliente está em  
execução 162  
ativar rastreio do cliente na linha de comandos 160  
cliente

cliente de backup-archive 160  
driver de dispositivo 150  
options 167  
problemas e limitações conhecidos 166  
servidor ou agente de armazenamento 121

rastreio de pilha

servidor ou agente de armazenamento 123

rastreio do driver de dispositivo

a partir de um shell de comando - AIX, Windows 152  
a partir do console do servidor/cliente admin 150

rastreio estendido 119, 120

recuperação de bancos de dados SQL individuais a partir de  
um backup da MV

acesso ao banco de dados de resolução de problemas 51  
exibindo bancos de dados SQL ativos 52  
mensagens 53  
nomes do banco de dados DBCS SQL 52  
resolvendo problemas 50  
salvando arquivos de manifesto VSS XML 54

recuperação de bancos de dados SQL individuais a partir de  
um backup da VMdeterminando o status de gravadores  
VSS 54

recursos da ajuda 1

recursos de acessibilidade 225

registros de resumo 63

RELABEL 61

reorganização

banco de dados 86

reorganização de banco de dados 86

reorganização de tabela 86

resolução de problemas

Operations Center 105, 106, 119

RESTORE DB

ANR2971E com o código SQL 83

erros comuns 85

variáveis de ambiente incorretas 82

restringindo a memória do DB2 78

## S

SAN

adaptadores de barramento de host 191

configuração 203

configuração do adaptador de barramento de host 192

configuração do comutador fibre channel 192

configuração entre dispositivos 194

configurações de porta do gateway 193

problemas de configuração 205

relatório de erro de link fibre-channel 194

suporte do fornecedor 205

scheduler

reinício de serviço do cliente 20

script gt 209

Secure Sockets Layer (SSL)

códigos de retorno gerais 213

determinando erros 110

senha autenticada por LDAP

resolução de problemas 11

- senha complexa
  - servidor de diretório LDAP 13
- senha do DB2
  - expirada 67
- senhas complexas
  - auditar o servidor de diretório LDAP 14
- Serviços do Windows
  - início/parada do serviço de servidor 73
- servidor
  - banco de dados 75
  - conjunto de armazenamento
    - alto uso de volume 101
    - colocação 101
    - comando COPY ACTIVATEDATA 102
    - gravação simultânea 102
    - mensagem de erro ANR0522W 100
    - não é possível armazenar dados 102
    - resolvendo problemas 99
  - conjunto de armazenamentos
    - resolvendo problemas 103
  - dicas de diagnóstico
    - erros de mudança nas opções do servidor e de criação de configurações 58
    - falha de conversão de página de códigos 152
    - falha em uma operação do cliente planejada 59
    - recriando o problema 57
    - resolvendo conexões com falha por cliente ou administradores 109
    - resolvendo erros de leitura ou gravação em um dispositivo 58
    - resolvendo problemas de espaço do servidor 59
    - verificando o log de atividades do servidor 57
  - erros de interrupção ou de loop 69
  - mensagens do processo 87
  - processo 87
- servidor de diretório LDAP
  - senha 13
- servidor de repositório do usuário externo
  - interrupção 70
- servidor ou agente de armazenamento
  - classes de rastreo 124
- sessões
  - atraso no cancelamento 107
- senhadores de rastreo do Daemon
  - cliente e diário 154
- senhadores de teste
  - VSS 46
- sintomas do processo
  - a migração não é executada 99
  - a migração usa apenas um processo 99
  - arquivos não expirados 98
- sistema de ajuda
  - CLI para servidor ou agente de armazenamento 3
  - clientes da GUI e da GUI da Web 3
  - dsmcutil 2
  - relatando um problema 3
  - servidor ou agente de armazenamento
    - mensagens 3
    - objetos do sistema 2
  - Windows 2
- sistema de arquivos criptografados 30
- solução de problemas
  - Operations Center 105, 119, 120
- SSL (Secure Sockets Layer)
  - códigos de retorno gerais 213
  - determinando erros 110

- status
  - Evento Planejado 18
- sugestões e dicas de armazenamento de dados
  - alterar a hierarquia de armazenamento 178
  - alterar as políticas do servidor 179
  - HELP 177
  - lendo ou gravando em um dispositivo 178
  - log de atividades do servidor 177
  - problema de backup ou cópia com o nó específico 179
  - recriar o problema 178
  - volume específico 180
- suporte para API
  - antes de entrar em contato com a IBM
    - arquivos a serem reunidos 36
    - informações a serem reunidas 35

## T

- tarefas ativas
  - atraso no cancelamento 107
- teclado 225
- tsmdiag 211, 212

## U

- upgrade
  - servidor manualmente 66
- utilitário tsmdiag 211
- utilitários
  - tsmdiag 211

## V

- Versão do DB2 78
- volume de mídia sequencial
  - fita 207
- Volume Shadow Copy Services
  - Windows 45
- VSS
  - ajuste da Microsoft 46
  - erros temporários 45
  - informações de diagnóstico da Microsoft 47
  - ntbackup.exe 48
  - programa de amostra vsreq.exe 48
  - rastreo 47
  - senhadores de teste 46
  - Windows 45

## W

- Windows
  - VSS 45





Número do Programa: 5725-W98  
5725-W99  
5725-X15

Impresso no Brasil