IBM Spectrum Protect
Version 8.1.0

Fehlerbestimmung

IBM Spectrum Protect
Version 8.1.0

Fehlerbestimmung

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 231 gelesen werden.

Diese Ausgabe bezieht sich auf Version 8, Release 1, Modifikation 0 von IBM Spectrum Protect (Produktnummern 5725-W98, 5725-W99, 5725-X15) und auf alle nachfolgenden Releases und Modifikationen, sofern in neuen Ausgaben nicht anders angegeben.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Spectrum Protect Version 8.1.0, Problem Determination Guide,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
TSC Germany
Kst. 2877
Dezember 2016

Inhaltsverzeichnis

Informationen zu dieser Veröffentlichung

Diese Veröffentlichung hilft Ihnen dabei, die Quelle von Problemen mit Servern und Clients in Ihrer IBM Spectrum Protect-Umgebung zu ermitteln.

Stellen Sie vor Verwendung dieser Veröffentlichung sicher, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Betriebssystem Ihres IBM Spectrum Protect-Servers und -Clients
- Auf dem Client- und Server-Computer installierte Übertragungsprotokolle

Zielgruppe

Dieses Handbuch richtet sich an alle Benutzer, die IBM Spectrum Protect verwalten. Die in ihm enthaltenen Informationen können darüber hinaus auch für Business Partner oder für Personen von Nutzen sein, die für die Unterstützung von IBM Spectrum Protect zuständig sind.

Sie sollten mit IBM Spectrum Protect und den Betriebssystemen vertraut sein, die für die IBM Spectrum Protect-Umgebung verwendet werden.

Veröffentlichungen

Die IBM Spectrum Protect-Produktfamilie umfasst IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for Databases und verschiedene andere Speicherverwaltungsprodukte von IBM®.

Die IBM Produktdokumentation finden Sie unter IBM Knowledge Center.

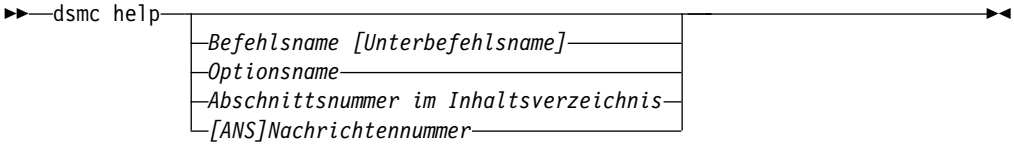
Kapitel 1. Hilfefunktionen

IBM Spectrum Protect stellt verschiedene Methoden zur Behebung von Problemen bereit, die Sie möglicherweise mit dem Server oder dem Client für Sichern/Archivieren haben.

Hilfe für Client für Sichern/Archivieren

Verwenden Sie den Befehl 'help', um Informationen zu Befehlen, Optionen und Nachrichten anzuzeigen. Wenn Sie den Befehl 'help' in der Anfangsbefehlszeile verwenden, wird kein Serverkontakt hergestellt und es ist kein Kennwort erforderlich.

Syntax



Wenn Sie den Befehl **HELP** ohne Argumente eingeben, wird das vollständige Inhaltsverzeichnis angezeigt. Die folgenden Parameter können Sie entweder mit dem Anfangsbefehl eingeben oder eingeben, wenn HELP eine Eingabeaufforderung anzeigt.

Parameter

Befehlsname [Unterbefehlsname]
Gibt einen Befehlsnamen und optional einen Unterbefehlsnamen bzw. die entsprechenden Abkürzungen an. Beispiel: **backup image** oder **b i**. In letzterem Fall sollte die Kombination eindeutig sein. Bei nicht eindeutigen Abkürzungen wird der erste Abschnitt der gesamten Hilfedatei angezeigt, die der Abkürzung entspricht. Dieser Parameter ist optional.

Optionsname
Gibt den Namen einer Option an. Beispiel: `domain` oder ***do***. Dieser Parameter ist optional.

Abschnittsnummer im Inhaltsverzeichnis
Gibt eine Abschnittsnummer im Inhaltsverzeichnis an. Beispiel: 1.5.3. Dieser Parameter ist optional.

[ANS]Nachrichtennummer
Gibt eine Nachrichtennummer mit oder ohne zugehöriges Präfix an. Beispiel: ans1036 oder 1036. Dieser Parameter ist optional. Der Bewertungscode muss in keinem Fall angegeben werden. Wird ans1036E eingegeben, werden keine Informationen gefunden.

Wichtig: Wenn Sie Argumente eingeben, die diesen Beschreibungen nicht entsprechen, werden möglicherweise unerwartete Ergebnisse (oder keine Ergebnisse) angezeigt. Wenn Sie mehr als zwei Argumente eingeben, wird Ihre Hilfeanforderung zurückgewiesen. Wenn ein Befehlsname und ein Optionsname identisch sind, bei-

spielsweise **incremental** (Befehl) und `incremental` (Option), können Sie Hilfe zu der Option nur aufrufen, wenn Sie die entsprechende Abschnittsnummer im Inhaltsverzeichnis eingeben.

Der angeforderte Hilfetext wird je nach der Anzahl der Anzeigezeilen in Ihrem Befehlsfenster in einem Abschnitt oder in mehreren Abschnitten angezeigt. Wenn der Anzeigebereich mit Zeilen gefüllt ist oder wenn das Ende des angeforderten Hilfetexts angezeigt wird, wird eine Eingabeaufforderung mit Anweisungen zu den möglichen Eingaben in der Eingabeaufforderung angezeigt. Soll mit der Anzeige von Text zu Ihrer aktuellen Auswahl fortgefahren werden, drücken Sie die **Eingabetaste** oder die Taste „d", um abwärts zu blättern. Um in der aktuellen Auswahl aufwärts zu blättern, drücken Sie die Taste „u" und drücken Sie die **Eingabetaste**. Drücken Sie die Taste „q", um die Hilfefunktion zu verlassen. Möglicherweise stehen weitere Auswahlmöglichkeiten zur Verfügung; lesen Sie also alle Anweisungen.

Für eine ordnungsgemäße Anzeige des Hilfetexts ist eine verwendbare Anzeigebreite von 72 Zeichen erforderlich. Eine Anzeigebreite von weniger als 72 Zeichen hat zur Folge, dass Sätze mit einer Breite von 72 Zeichen in der nächsten Zeile fortgesetzt werden. Dies kann dazu führen, dass nicht der Anfang, sondern ein Abschnitt in der Mitte des Hilfetexts angezeigt wird. Die nicht angezeigten Zeilen können mit der Blätterfunktion der Datenstation angezeigt werden.

Auf Hilfe für das Konfigurationsdienstprogramm für den Client-Service (`dsmcutil`) zugreifen

Windows

Um Hilfeinformationen für das IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service aufzurufen, müssen Sie den Befehl **DSMCUTIL HELP** ausgeben.

Wenn Sie den Befehl **DSMCUTIL HELP** ausgeben, werden die Hilfeinformationen im Hilfedienstprogramm von Windows angezeigt.

Hilfe für Server oder Speicheragenten

Der Server und der Speicheragent verfügen beide über eine Hilfefunktion. Die Hilfefunktion stellt Beschreibungen und Syntax für Serverbefehle und eine vollständige Beschreibung der Servernachrichten zur Verfügung.

Auf Server- oder Speicheragentenhilfe für Befehle zugreifen

Geben Sie den Befehl **HELP** aus, um auf die Hilfe für den Server oder den Speicheragenten zuzugreifen.

Um Befehlszeilenhilfe für Serverbefehle anzuzeigen, die eindeutige Namen haben, können Sie `help` *`Befehlsname`* eingeben, wobei *Befehlsname* der Name des Serverbefehls ist, für den Informationen gewünscht werden. Soll beispielsweise für den Befehl **REGISTER NODE** Hilfe angezeigt werden, geben Sie `help` *`register node`* ein. Befehlssyntax und Parameterbeschreibungen werden in der Ausgabe angezeigt.

Sie können auch `help`, gefolgt von der Abschnittsnummer für den Befehl eingeben. Abschnittsnummern sind im Inhaltsverzeichnis der Befehlszeilenhilfe aufgelistet, z. B.:

```
3.0 Verwaltungsbefehle
  3.46 REGISTER
     3.46.1 REGISTER ADMIN (Administrator registrieren)
     3.46.2 REGISTER LICENSE (Neue Lizenz registrieren)
     3.46.3 REGISTER NODE (Knoten registrieren)
```

Soll Hilfe für den Befehl **REGISTER NODE** angezeigt werden, geben Sie Folgendes ein:

```
help 3.46.3
```

Verwenden Sie Abschnittsnummern, um Befehlszeilenhilfe für Unterbefehle anzuzeigen. **DEFINE DEVCLASS** ist ein Beispiel für einen Befehl, der Unterbefehle hat. Sie können z. B. den Befehl **DEFINE DEVCLASS** für die Einheitenklasse 3590 und für die Einheitenklasse 3592 angeben:

```
3.0 Verwaltungsbefehle
  ...
  3.13.10 DEFINE DEVCLASS (Einheitenklasse definieren)
      3.13.10.1 DEFINE DEVCLASS (Einheitenklasse 3590 definieren)
      3.13.10.2 DEFINE DEVCLASS (Einheitenklasse 3592 definieren)
      ...
```

Soll Hilfe für den Befehl **DEFINE DEVCLASS** für die Einheitenklasse 3590 angezeigt werden, geben Sie Folgendes ein:

```
help 3.13.10.1
```

Auf Hilfe für Nachrichten zugreifen

Geben Sie den Befehl HELP aus, um auf die Hilfe für Nachrichten zuzugreifen.

Geben Sie den folgenden Befehl aus, um Hilfe für eine Servernachricht abzurufen: HELP *Nachrichtennummer*. Hierbei steht *Nachrichtennummer* für die Nachricht, für die Sie Informationen benötigen. Wenn Sie die Nachrichtennummer ohne das Nachrichtenpräfix angeben, z. B. HELP 0445, wird das Nachrichtenpräfix ANR angenommen und die Hilfeinformationen für Nachricht ANR0445W werden angezeigt. Wird die Nachrichtennummer mit dem Präfix angegeben, z. B. HELP ANR0445, werden die Hilfeinformationen für diese Nachricht angezeigt. Geben Sie HELP ANR0445 aus, um die folgende Beispielausgabe für diese Nachricht aufzurufen:

```
ANR0445W Protokollfehler in Sitzung Sitzungsnummer für Knoten Name des Client-Knotens
(Clientplattform) - maximale Transaktionsgröße überschritten.
Erläuterung: Der Server hat in der angegebenen Sitzung einen Protokollfehler
erkannt, da der Client versucht hat, mehr als die maximale Anzahl
Datenbankaktualisierungsoperationen in einer einzelnen
Datenbanktransaktion zusammenzufassen.
Systemaktion: Der Server beendet die Clientsitzung.
Benutzeraktion: Den Programmierfehler in dem Clientprogramm korrigieren, wenn
es von der Installation unter Verwendung von WDSF-Verben geschrieben wurde.
Andernfalls den Kundendienst benachrichtigen.
```

Hilfe der Befehlszeilenschnittstelle für den Client

Die Befehlszeilenclientschnittstelle verfügt über eine Hilfefunktion, die Beschreibungen und Syntax für Clientbefehle und -optionen sowie eine vollständige Beschreibung der Clientnachrichten zur Verfügung stellt.

Hilfeinformationen für den GUI-Client und den Web-GUI-Client sind über den Menüpunkt **Hilfe** verfügbar.

Problem mit einem Hilfethema melden

Wenn Sie ein Problem mit der Hilfefunktion melden möchten, müssen Sie zuerst bestimmte Informationen sammeln.

1. Zeichnen Sie auf, auf was Sie geklickt haben, um die Hilfe abzurufen. Wenn Sie beispielsweise auf das Fragezeichen für ein Portal geklickt haben, zeichnen Sie den Namen des Portals auf.
2. Zeigen Sie die Quelle des Popup-Hilfefensters an. Bei den meisten Browsern wird durch Klicken mit der rechten Maustaste ein Menü aufgerufen, das eine Option zum Anzeigen der Quelle enthält. Wählen Sie **Quelltext anzeigen** aus, um den HTML-Quellcode für dieses Fenster anzuzeigen. Notieren Sie den Titel dieses Fensters. Hierbei handelt es sich um die URL oder den Namen der Datei, die die Hilfefunktion anzuzeigen versucht.

Kapitel 2. Clientprobleme beheben

Die Fehlerbehebung für die Clientanwendung kann die Herstellung der Verbindung zum Server, die Änderung der Maßnahmeneinstellungen, die Reproduzierung des Fehlers und verschiedene andere mögliche Optionen einbeziehen.

Fehlernachrichten untersuchen

Sie können die während der Programmausführung generierten Fehlernachrichten untersuchen, um möglicherweise auftretende Probleme zu beheben.

Wenn die IBM Spectrum Protect-Client-Option `QUIET` festgelegt ist, wird das Anzeigen aller Nachrichten in der Ausgabe am Bildschirm unterdrückt. In den Protokolldateien werden jedoch weiterhin alle Nachrichten protokolliert. Das Inaktivieren der Option `QUIET` kann die Fehlerbehebung vereinfachen, weil Sie die Nachrichten in der Anzeige sehen können, sobald sie ausgegeben werden.

Suchen Sie nach Nachrichten `ANSnnnnx`, die in der Konsole ausgegeben werden. Nachrichten werden ebenfalls protokolliert. Schedulernachrichten werden in der Datei `dsmsched.log` protokolliert. Clientnachrichten werden in der Datei `dsmerror.log` protokolliert. Beschreibungen der Nachrichten und API-Rückkehrcodes werden in Nachrichten, Rückkehrcodes und Fehlercodes bereitgestellt. Für Systemnachrichten steht außerdem eine Onlinehilfe zur Verfügung. Um bei Verwendung des Befehlszeilenclients die Onlinehilfe für eine Nachricht aufzurufen, geben Sie **`HELP`** *ANS_nnnnx* ein. Hierbei steht *nnnn* für die Nachrichtennummer und *x* für den Nachrichtentyp.

Nachrichten im Serveraktivitätenprotokoll untersuchen

Verwenden Sie den Befehl **`QUERY ACTLOG`**, um die Serveraktivitätenprotokolldatei und die Nachrichten anzuzeigen, die für diese Clientsitzung ausgegeben wurden.

Die Nachrichten im Serveraktivitätenprotokoll können weitere Informationen zu den Symptomen des Fehlers oder Informationen zur tatsächlichen Ursache des Fehlers bereitstellen, der vom Client festgestellt wurde.

Identifizieren, wann und wo der Fehler auftreten kann

Fehler bei der Clientverarbeitung treten häufig nur auf, wenn bestimmte Operationen zu bestimmten Zeiten ausgeführt werden, oder sie treten nur auf bestimmten Client-Computern auf.

Um weiter einzugrenzen, wann und wo ein Fehler auftritt, beantworten Sie die folgenden Fragen:

- Tritt dieser Fehler bei einem einzelnen Client, bei einigen Clients oder bei allen Clients für einen bestimmten Server auf?
- Tritt dieser Fehler bei allen Clients auf, die unter einem bestimmten Betriebssystem ausgeführt werden?
- Tritt dieser Fehler bei bestimmten Dateien, bei Dateien in einem bestimmten Verzeichnis, bei Dateien auf einem bestimmten Laufwerk oder bei allen Dateien auf?

- Tritt dieser Fehler bei Clients in einem bestimmten Netz, Teilnetz oder in allen Teilen des Netzes auf?
- Tritt dieser Fehler nur für den Befehlszeilenclient, den GUI-Client oder den Web-Client auf?
- Schlägt IBM Spectrum Protect immer fehl, wenn dieselbe Datei oder dasselbe Verzeichnis verarbeitet wird, oder ist dies von Ausführung zu Ausführung unterschiedlich?

Fehler reproduzieren

Wenn Sie einen Fehler im Rahmen der Fehlerbestimmung reproduzieren, versuchen Sie, die Auswirkungen zu minimieren, die der Prozess auf IBM Spectrum Protect hat.

Sie können der IBM Spectrum Protect-Unterstützung helfen, indem Sie die Komplexität der Umgebung verringern, in der der Fehler reproduziert werden soll. Die folgenden Optionen können verwendet werden, um die Komplexität der Umgebung zu verringern:

- Verwenden Sie eine minimale Optionsdatei, die nur aus `TCPSERVERADDRESS`, `TCPPORT` und `NODENAME` besteht.
- Wenn der Fehler bei einer Datei während der Teilsicherung auftritt, versuchen Sie, den Fehler mit einer selektiven Sicherung nur mit dieser Datei zu reproduzieren.
- Wenn der Fehler während eines geplanten Ereignisses auftritt, versuchen Sie den Fehler zu reproduzieren, indem Sie den Befehl manuell ausführen.

Dokumentation erfassen, um Probleme mit der Clientanwendung zu beheben

Das Unterstützungsteam bei IBM kann ein Problem besser beheben, wenn Sie relevante Dokumentation bereitstellen. Der Client für Sichern/Archivieren erstellt Informationen in einer Reihe von verschiedenen Quellen.

Tipp: IBM Spectrum Protect hat eine integrierte Hilfefunktion innerhalb der Clientbefehlszeile. Geben Sie den Befehl **`dsmc help`** aus, um auf die Hilfefunktion des Befehlszeilenclients zuzugreifen. Die Hilfefunktion ist eine menügeführte Schnittstelle mit Informationen, die die Befehlsreferenz, Optionsreferenz und erweiterte Informationen zu Clientnachrichten umfassen.

Clientprobleme und Konfigurationsinformationen können sich in einem oder in mehreren der folgenden Dokumente befinden:

- Fehlerprotokoll. Die Clientfehlerprotokolldatei ist `dsmerror.log`.
- Schedulerprotokoll. Das Fehlerprotokoll für den Client-Scheduler ist `dsmsched.log`.
- Web-Clientprotokoll. Das Fehlerprotokoll für den Web-Client ist `dsmwebcl.log`.
- Optionsdateien. Die Informationen zu den Optionen, die für die Clients festgelegt sind, können die Fehlerbehebung und die Problemlösung vereinfachen. Viele dieser Informationen befinden sich in den folgenden Dateien:
  - Clientoptionsdatei (`dsm.opt`). Diese Datei ist für alle Clients auf allen Betriebssystemen vorhanden.
  - Clientsystemoptionsdatei (`dsm.sys`). Diese Datei wird nur auf AIX-, Linux- und Mac OS X-Clients verwendet.

  - Einschluss-/Ausschlussdatei. Diese Datei enthält die Objekte, die bei Clientoperationen ein- bzw. ausgeschlossen werden sollen. Ihre Position ist durch die Clientoption `inclexcl` definiert.
- Tracedaten. Falls die Tracefunktion aktiv war, kann die Datei, in der die Tracedaten enthalten sind, dem Support zur Verfügung gestellt werden.
- Anwendungsspeicherauszug. Wenn die Ausführung des Clients für Sichern/Archivieren unerwarteterweise gestoppt wird, generieren viele Plattformen einen Anwendungsspeicherauszug. Das Betriebssystem stellt den Anwendungsspeicherauszug bereit.
- Hauptspeicherauszug. Wenn der Client für Sichern/Archivieren gestoppt wird, kann ein Hauptspeicherauszug generiert werden, der bei der Fehlerdiagnose helfen kann. Der Typ des Systems bestimmt, wie der Hauptspeicherauszug erfolgt, und das Betriebssystem stellt den Hauptspeicherauszug bereit.

Der Befehl **DSMC QUERY SYSTEMINFO** ist verfügbar, mit dem die meisten dieser Informationen in der Datei `dsminfo.txt` erfasst werden. Die folgenden Elemente können Ihnen helfen, IBM Spectrum Protect-Probleme zu bestimmen:

- Eine Liste der gesamten Software, die auf dem Clientsystem installiert ist. Der Client kann Probleme aufgrund von Interaktionen mit anderer Software auf dem Computer oder aufgrund der Wartungsstufen der Software feststellen, die der Client verwendet.
- Auf dem Server definierte Clientoptionsgruppen, die für diesen Clientknoten gelten. Geben Sie den Befehl **QUERY CLOPTSET** aus, um nach den Clientoptionsgruppen zu suchen.
- Serveroptionen. Es gibt eine Reihe von Serveroptionen, die verwendet werden, um die Interaktion zwischen dem Client für Sichern/Archivieren und dem Server zu steuern. Ein Beispiel für eine solche Serveroption ist `TXNGROUPMAX`.
- Informationen zu diesem Knoten, wie er für den Server definiert ist. Um diese Informationen zu erfassen, geben Sie den Befehl **QUERY NODE** *Knotenname* **F=D** unter Verwendung eines Verwaltungsclients aus, der mit dem Server verbunden ist.
- Zeitplandefinitionen für die Zeitpläne, die für diesen Knoten gelten. Die Zeitplandefinitionen können vom Server abgefragt werden, wenn Sie den Befehl **QUERY SCHEDULE** ausgeben.
- Die Maßnahmeninformationen, die für diesen Knoten auf dem Server konfiguriert sind. Die Maßnahmeninformationen können vom Server abgefragt werden, wenn Sie den Befehl **QUERY DOMAIN**, **QUERY POLICYSET**, **QUERY MANAGEMENTCLASS** oder **QUERY COPYGROUP** ausgeben.

Ursache für nicht erfolgten Start des Programms `dsmc`, `dsmadmc`, `dsm` oder `dsmj` ermitteln

Der Client für Sichern/Archivieren verwendet die Programme **dsmc**, **dsmadmc**, **dsm** oder **dsmj** in seiner Startprozedur. Wenn eines dieser Programme nicht gestartet wird, wird der Client für Sichern/Archivieren nicht gestartet.

Die Programme **dsmc**, **dsmadmc**, **dsm** oder **dsmj** sind wie folgt definiert:

dsmc Der Befehlszeilenclient für Sichern/Archivieren.

dsmadmc
Der Verwaltungsbefehlszeilenclient.

Windows **dsm**

AIX Linux **dsmj**

Die grafische Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren. Die Oracle Java™-Laufzeitversion wird beim ersten Start der Java-GUI überprüft. In einigen Fällen wird diese Überprüfung nicht ordnungsgemäß ausgeführt, und der Start von **dsm** oder **dsmj** kann mit einer Nachricht „falsche Nummer" fehlschlagen.

Die Verarbeitung wird gestoppt und die folgende Nachricht wird angezeigt, wenn das Programm **dsmc**, **dsmadmc**, **dsm** oder **dsmj** nicht gestartet wird:

```
ANS1398E Initialisierungsfunktionen können eines der IBM Spectrum Protect-Protokolle
oder eine verwandte Datei nicht öffnen: dsmerror.log. Fehlernummer = 13,
Die Dateizugriffsberechtigungen erlauben nicht die angegebene Aktion.
```

Hinweis: Die Datei `dsmerror.log` wird nur als Beispieldatei in der Nachricht verwendet.

Clientanwendungen werden nicht ausgeführt, wenn sie nicht in eine Protokolldatei schreiben können, und das System verweigert den Schreibzugriff auf die in der Nachricht angegebene Protokolldatei. Wenn die Protokolldatei nicht vorhanden ist, wird sie mit Standardberechtigungen erstellt. Es gelten die folgenden Regeln:

1. Der Name und das Verzeichnis, die mit der Option `ERRORLOGNAME` angegeben sind, werden verwendet.
2. Ist die Option nicht vorhanden, wird der Name `dsmerror.log` in dem Verzeichnis verwendet, das in der Umgebungsvariablen **DSM_LOG** (falls vorhanden) angegeben ist. Andernfalls wird der Name `dsmerror.log` im aktuellen Arbeitsverzeichnis verwendet.

Die folgenden Hinweise gelten, wenn Standardberechtigungen verwendet werden:

- Eine Protokolldatei, die vom Rootbenutzer erstellt wird, ist für alle anderen Benutzer nicht beschreibbar
- Der Rootbenutzer muss die geeigneten Berechtigungen oder Zugriffssteuerungslisten definieren, um die freie Verwendung der Clientanwendung durch alle Benutzer, die die Clientanwendung verwenden müssen, zu ermöglichen

Wenn die Protokolldatei erfolgreich erstellt wird, ist das Ergebnis einer fehlerfreien Sitzung eine Protokolldatei mit einer Nulllänge (leere Protokolldatei).

Der Client versucht nicht, Protokolldateien im Stammverzeichnis zu erstellen. Die Nachricht ANS1398E wird angezeigt, wenn die Methode in der ersten Regel angibt, dass die Protokolldatei im Stammverzeichnis erstellt werden soll.

Wenn eine Protokolldatei vorhanden ist und lokalisiert werden kann, verwendet IBM Spectrum Protect die Methode aus der ersten Regel. Die Protokolldatei kann sich auch im Stammverzeichnis befinden, wenn Sie die entsprechende Auswahl treffen. Unabhängig davon, welche Berechtigungen Sie erteilen, wird diese Protokolldatei vom IBM Spectrum Protect-Code aufbewahrt.

Erstellen Sie Ihre Protokolldatei vor der ersten Verwendung und stellen Sie sicher, dass alle Nutzungsberechtigte Schreibzugriff auf die Protokolldatei haben. Definieren Sie die Option `ERRORLOGNAME` oder die Umgebungsvariable **DSM_DIR**, um Ihre vordefinierte Protokolldatei anzugeben.

Achtung: Ein Fehler in der Systemprotokolldatei gibt an, dass Sie nicht in die Datei `dsmerror.log` schreiben können. Bestimmte IBM Spectrum Protect-Hintergrundanwendungen werden möglicherweise aufgrund von Schreibfehlern für die Datei `dsmerror.log` nicht gestartet. Wenn diese Fehler auftreten, wird eine Reihe von Fehlern in der Windows-Systemereignisprotokolldatei bzw. bei anderen Betriebssystemen in der Systemprotokolldatei aufgezeichnet.

Windows Beispiel:

```
C:\Programme\Tivoli\Tsm\baclient>net start "TSM Sched"
Der Serverzeitplanungsservice wird gestartet.
Der Serverzeitplanungsservice konnte nicht gestartet werden.
Ein servicespezifischer Fehler ist aufgetreten: 12.
```

AIX Linux Mac OS X Zusätzliche Konfigurationsschritte sind für Benutzer ohne Rootberechtigung erforderlich, damit sie IBM Spectrum Protect-Anwendungen oder IBM Spectrum Protect for Data Protection-Anwendungen ausführen können. Sie erhalten die Fehlernachricht ANS1398E, wenn Sie versuchen, IBM Spectrum Protect-Anwendungen mit einer vom Root bereits generierten Fehlerprotokolldatei mit Standardberechtigungen auszuführen. Für Data Protection-Clients erhalten Sie möglicherweise nur einen IBM Spectrum Protect-API-Fehler. Nachfolgend finden Sie eine Methode zum Definieren von `dsmerror.log` für die Verwendung durch Benutzer ohne Rootberechtigung:

1. Definieren Sie **`ERRORLOGNAME`** in `dsm.sys`. Beispiel: `errorLogName /var/msgs/tsm/dsmerror.log`
2. Generieren Sie **`dsmerror.log. dsmc q sess`**
3. Ändern Sie die Berechtigungen für `dsmerror.log`, um das Schreiben für alle Benutzer zu ermöglichen. `chmod 666 /var/msgs/tsm/dsmerror.log`

Fehler für Clientoptionsgruppen beheben

Mit Clientoptionsgruppen können Administratoren zusätzliche Optionen angeben, die möglicherweise in der Optionsdatei des Clients für Sichern/Archivieren nicht enthalten sind. Der Client für Sichern/Archivieren verwendet diese Optionen während eines Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufprozesses.

Ein Administrator für IBM Spectrum Protect kann eine Gruppe von Clientoptionen erstellen, die von einem Clientknoten in IBM Spectrum Protect verwendet werden sollen. Die Clientoptionen werden auf dem IBM Spectrum Protect-Server definiert. Die in der Clientoptionsgruppe angegebenen Clientoptionen werden zusammen mit der Clientoptionsdatei verwendet.

Die Reihenfolge, in der die Optionen verarbeitet werden, kann gesteuert werden. Es können mehrere Optionen definiert und dann den Optionen Folgenummern zugeordnet werden. Diese Optionen werden dann in der Reihenfolge von unten nach oben verarbeitet. Das folgende Beispiel zeigt die Optionen **`INCLEXCL`**:

```
Option            Folge-     Über-      Optionswert
                  nummer     schreiben
------------      --------   --------   ---------------------------------
INCLEXCL            0          No        exclude 'sys:\backup\*'
INCLEXCL            1          No        include 'sys:\system\*'
INCLEXCL            2          No        include 'sys:\tmp\*'
```

Diese Reihenfolge resultiert im Ausschluss aller Dateien im Pfad `sys:\backup\*`, während die Dateien in den Pfaden `sys:\system\*` und `sys:\tmp\*` gesichert wer-

den.

Szenarios für die Fehlerbehebung bei Clientoptionsgruppen

Verwenden Sie Clientoptionsgruppen, um verschiedene Probleme zu beheben, beginnend mit kritischen Umgebungen, in denen die Zurückschreibung eine hohe Priorität hat, bis hin zur Verwendung einer Datenbank, die nicht gestoppt wird.

Tipp: Traceeinstellungen für die Clientoptionsgruppen werden in der IBM Spectrum Protect-Optionsdatei für alle Clients für Sichern/Archivieren angegeben.

Die folgenden Szenarios zeigen, wie Sie die Clientoptionsgruppen nutzen können.

Szenario 1: Umgebung, in der die Zurückschreibung eine hohe Priorität hat.

Verwenden Sie die Option `COLLOCATEBYFILESPEC`, damit alle Dateispezifikationsdaten auf möglichst wenig Bänder gespeichert werden. Die Zurückschreibungsverarbeitung wird verbessert, da weniger Bandladevorgänge erforderlich sind. Sie möchten nicht, dass der Client diese Option überschreibt. Geben Sie den folgenden Serverbefehl aus:

```
Define cloptset crit_rest description="Optionsgruppen für kritische Zurückschreibung"
Define clientopt crit_rest collocatebyfilespec yes force=yes
Update node dale cloptset=crit_rest
```

Szenario 2: Verwendung von Workstations in einem langsamen Netz mit begrenztem Speicherbereich für Daten auf dem Server.

Verwenden Sie die Komprimierungsoption, um das gesendete und gespeicherte Datenvolumen zu begrenzen. Geben Sie den folgenden Serverbefehl aus:

```
Define cloptset space_rest description="Optionsgruppen für Speicherbeschränkung"
Define clientopt space_rest compressalways no force=yes
Define clientopt space_rest compression yes force=yes
Update node mark cloptset=space_rest
```

Szenario 3: Verwendung einer Datenbank, die nicht gestoppt wird.

Ein Problem mit der Datenbank ist vorhanden, da die Dateien offen sind und der Server sie nicht sichern kann. Schließen Sie alle Dateien und Unterverzeichnisse von IBM Spectrum Protect-Sicherungen aus und fügen Sie die Dateien und Unterverzeichnisse der vorhandenen Clientoptionsgruppe „`space_rest`" hinzu. Geben Sie den Befehl **`EXCLUDE DIR`** aus und geben Sie den Verzeichnispfad an, der ausgeschlossen werden soll. Geben Sie den folgenden Serverbefehl aus:

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

Szenario 4: Ausführung von Sicherungen in einem schnellen Netz und bestmögliche Verwendung von Clientressourcen.

Setzen Sie die Option `RESOURCEUTILIZATION` auf den maximalen Wert. Geben Sie den folgenden Serverbefehl aus:

```
Define cloptset unix_srv description="Optionsgruppen für UNIX-Server"
Define clientopt unix_srv resourceutilization 10 force=yes
```

Probleme beim Kennwortablauf beheben

Falls Sie einen Clientauthentifizierungsfehler empfangen, kann dieser auf ein abgelaufenes Kennwort zurückzuführen sein. Der Kennwortablauf gilt nicht für Knoten- oder Administratorkennwörter, die mit einem LDAP-Verzeichnisserver authentifiziert werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Zeitraum für den Kennwortverfall zu ändern:

1. Um die Kennwortablaufdauer für einen bestimmten Knoten zu ändern, geben Sie den Serverbefehl **UPDATE NODE** mit der Option **PASSEXP**=*n* aus; dabei gibt *n* die Anzahl Tage an. Mit dem Wert 0 wird der Kennwortablauf inaktiviert.

   Wenn ein Windows-Clientknoten nach der Umbenennung keine Verbindung zum Server herstellen kann, überprüfen Sie, ob der Knotenname sowohl in der Clientoptionsdatei als auch in der Windows-Registrierungsdatenbank geändert wurde. Wenn der Client-Scheduler als Vordergrundprozess ausgeführt wird und den Befehl **DSMC SCHED** verwendet, verwendet IBM Spectrum Protect den Knotennamen in der Clientoptionsdatei, um die Verbindung zum Server herzustellen. Wenn der Scheduler jedoch als Windows-Dienst ausgeführt wird, verwendet IBM Spectrum Protect den Knotennamen in der Windows-Registrierungsdatenbank.
2. Geben Sie für den Windows-Client den Befehl **DSMCUTIL UPDATE SCHEDULE** aus, um die folgenden Ergebnisse zu erzielen:
   - Geben Sie den Parameter *node* an, um festzulegen, wie der Knotenname geändert werden soll, der mit dem IBM Spectrum Protect-Scheduler-Service unter Windows verwendet wird.
   - Geben Sie den Parameter *validate:yes* an, um die Verbindung zum IBM Spectrum Protect-Server für die Authentifizierung herzustellen (und das aktualisierte Kennwort zu speichern).

Probleme bei mit LDAP authentifizierten Kennwörtern beheben

Die meisten bei der Kennwortauthentifizierung entstehenden Probleme können auf die Verbindung zwischen dem IBM Spectrum Protect-Server und dem LDAP-Verzeichnisserver zurückgeführt werden.

Diese Dokumentation bezieht sich auf die LDAP-Authentifizierungsmethode, die für Server vor Version 7.1.7 und von IBM Security Directory Server-Benutzern verwendet wird. Weitere Informationen zu dieser Methode finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Bevor Sie das mit LDAP authentifizierte Kennwort verwenden können, müssen Sie den LDAP-Verzeichnisserver so konfigurieren, dass er mit dem IBM Spectrum Protect-Server kommuniziert. Stellen Sie sicher, dass die Zugriffssteuerungsliste auf dem LDAP-Verzeichnisserver einem Benutzer (LDAPUSER) über den Basis-DN eine umfassende Berechtigung erteilt.

Konfiguration für die Kennwortauthentifizierung prüfen

Falls Sie den Server für die Authentifizierung von Kennwörtern mit einem LDAP-Verzeichnisserver konfiguriert haben und Fehler empfangen, prüfen Sie die Konfigurationsschritte. Sie müssen sicherstellen, dass der IBM Spectrum Protect-Server und der LDAP-Verzeichnisserver ordnungsgemäß konfiguriert wurden.

Vorgehensweise

1. Öffnen Sie die Optionsdatei `dsmserv.opt` und suchen Sie nach der Option **LDAPURL**, die den Server und den Basis-DN enthält. Sie können weitere Werte zur Option **LDAPURL** hinzufügen, wobei jeder URL-Wert bis zu 1024 Zeichen umfassen kann. Die Portnummer ist optional. Die Standardportnummer ist 389. Jede URL-Konfiguration muss die folgenden Werte enthalten:
   - Name eines LDAP-Verzeichnisservers.
   - Basis-DN des Namensbereichs oder Suffix, der vom LDAP-Verzeichnisserver verwaltet wird. Das Format des DN muss dem ausgewählten Verzeichnisserver entsprechen.

   Die Option **LDAPURL** muss die folgenden Spezifikationen einhalten:
   - Befolgen Sie bei der Angabe mehrerer URLs die folgenden Richtlinien:
     - Jede URL muss sich in einer separaten Zeile befindet.
     - Jede URL muss auf ein anderes externes Verzeichnis verweisen und alle externen Verzeichnisse müssen dieselben Daten enthalten.
   - Jede URL muss mit der Angabe `ldap://` beginnen.

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

   Die angegebene URL kann keine sichere URL sein, also nicht mit der Angabe `ldaps://` beginnen.
2. Zeigen Sie die Einstellungen für **LDAPUSER** oder **LDAPPASSWORD** an, indem Sie den Befehl **QUERY STATUS** ausgeben. Definieren Sie die Option **LDAPUSER**, also den Benutzer, der anschließend Einträge hinzufügen oder entfernen sowie Kennwörter ändern oder zurücksetzen kann. Falls die Option **LDAPUSER** nicht definiert ist, geben Sie den Befehl **SET LDAPUSER** aus, um den Administrator des LDAP-Verzeichnisservers zu definieren.

   Wichtig: Falls der Wert für den Parameter **LDAPUSER** Sonderzeichen enthält, schließen Sie den Wert in Anführungszeichen ein. Beispiel:
   ```
   set ldapuser "cn=bill cook,cn=users,dc=storage,dc=dallas,dc=gov"
   ```
3. Zeigen Sie die Einstellungen für **LDAPUSER** oder **LDAPPASSWORD** an, indem Sie den Befehl **QUERY STATUS** ausgeben. Falls kein Kennwort definiert ist, legen Sie ein Kennwort für **LDAPUSER** fest, indem Sie den Befehl **SET LDAPPASSWORD** ausgeben.

   In einem Kennwort können Sie die folgenden Zeichen verwenden:
   ```
   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 . ! @ # $ % ^ & * _ - + = ` ( )
   | { } [ ] : ; < > , ? / ~
   ```

   Voraussetzung: Falls Sie beim Ausgeben des Befehls **SET LDAPPASSWORD** Sonderzeichen verwenden, schließen Sie diese in Anführungszeichen ein. Beispiel:
   ```
   set ldappassword "Pa$$=w0rd"
   ```

IBM Spectrum Protect-Server akzeptiert LDAPPASSWORD nicht

Falls Sie die Warnung empfangen, dass die Option LDAPPASSWORD ungültig ist, hängt das Problem nicht zwangsläufig mit dem Kennwort zusammen.

Falls Sie einen Befehl **SET LDAPPASSWORD** ausgeben und die Fehlernachricht ANR3114E oder ANR3116E empfangen, ist IBM Spectrum Protect möglicherweise nicht ordnungsgemäß konfiguriert. Untersuchen Sie alle etwaigen Servernachrichten, die etwa zum Zeitpunkt der Nachricht ANR3114E oder ANR3116E ausgegeben wurden, um die Ursache der Fehler zu ermitteln. Häufig ist das Problem darauf zurückzuführen, dass für den Befehl **SET LDAPUSER** ein falscher Wert festgelegt wurde. Der Benutzer muss im Format für den definierten Namen (DN) angegeben werden. Beispiel:

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

Falls der Wert nicht dem DN entspricht, wird **LDAPUSER** nicht definiert und es kann kein Wert für die Option LDAPPASSWORD festgelegt werden. Ein definierter Name (DN) besteht normalerweise aus einer durch Kommas getrennten Liste von Paaren aus Namensattributen und Werten. Die gemeinhin verwendeten Namensattribute sind in der folgenden Liste aufgeführt:

- cn (allgemeiner Name)
- uid (Benutzer-ID)
- ou (Organisationseinheit)
- dc (Domänenkomponente)
- o (Organisation)
- c (Land)

Beispiel:

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

Probleme mit dem LDAP-Verzeichnisserver beheben

Falls bei der Kennwortauthentifizierung Probleme auftreten, müssen Sie sicherstellen, dass Sie alle Konfigurationsschritte ordnungsgemäß durchgeführt haben. Sie müssen unter anderem dafür sorgen, dass der Basis-DN auf dem LDAP-Verzeichnisserver definiert wurde und dass die Option **LDAPURL** definiert ist.

Nachdem Sie den Tivoli Storage Manager-Server Version 6.3.3 oder höher oder den IBM Spectrum Protect-Server Version 7.1.3 oder höher installiert haben, müssen Sie den LDAP-Verzeichnisserver für die Kommunikation mit dem Server konfigurieren.

Falls Verbindungsprobleme auftreten, führen Sie die folgenden Schritte mit einem LDAP-Dienstprogramm wie beispielsweise `ldapsearch` oder `ldp.exe` aus:

1. Testen Sie die DNS-Vorwärtssuche und die umgekehrte DNS-Suche des LDAP-Serversystems auf dem Serversystem.
2. Testen Sie die Netzverbindung zwischen dem Betriebssystem des Servers und dem Betriebssystem des LDAP-Verzeichnisservers.
3. Stellen Sie mit dem Hostnamen und dem Anschluss, die Sie in der Option **LDAPURL** angegeben haben, eine Verbindung zum LDAP-Verzeichnisserver her.
4. Bauen Sie eine Verbindung mit Transport Layer Security (TLS) auf, indem Sie die Option **StartTLS** ausgeben.

5. Verwenden Sie die Authentifizierung durch einfaches Binden, um die Authentifizierung mit den Parametern durchzuführen, die Sie für **LDAPUSER** und **LDAPPASSWORD** definiert haben.
6. Durchsuchen Sie den LDAP-Verzeichnisserver nach dem Basis-DN, den Sie in der Option **LDAPURL** angegeben haben.

Ein LDAP-Serveradministrator könnte Authentifizierungsprobleme im Zusammenhang mit dem LDAP-Verzeichnis wie folgt mithilfe des Dienstprogramms **ldapsearch** beheben:

Mit OpenLDAP (die Zertifikatsdatei wird mit der Option TLS_CACERT in der Datei ldap.conf angegeben)
Ohne SSL/TLS

```
ldapsearch -H <Hostname>
-D <LDAPUSER> -W -s base -b
<Basis-DN aus LDAPURL> -v -x objectclass="*"
```

Mit SSL/TLS

```
ldapsearch -H <Hostname>
 -D <LDAPUSER> -W -s base -b
<Basis-DN aus LDAPURL> -v -x -ZZ objectclass="*"
```

Mit dem LDAP-Client (wird mit AIX installiert oder von ibm.com heruntergeladen)
Ohne SSL/TLS

```
ldapsearch -h <Hostname>
-D <LDAPUSER>  -w ? -s base -b
<Basis-DN aus LDAPURL> -v objectclass="*"
```

Mit SSL/TLS

```
ldapsearch -h <Hostname>
-D <LDAPUSER> -w ? -s base -b
<Basis-DN aus LDAPURL> -v -Y -x -K "cert.kdb" objectclass="*"
```

Bei den obigen Befehlen gelten die folgenden Parameter:

- *Hostname*: Die URL aus der Option **LDAPURL**, z. B.
  `ldap://ldap.ibm.com:389/`
- *LDAPUSER*: Die Parameter aus dem Befehl **SET LDAPUSER**, z. B.
  `cn=tsmserver,cn=users,dc=ibm,dc=com`
- *Basis-DN aus LDAPURL*: Der Basis-DN aus der Option **LDAPURL**, z. B.
  `"OU=tsm,DC=ibm,DC=com"`

Probleme mit gesperrten Knoten und Administratoren beheben

Die Kennwörter für die Authentifizierung beim LDAP-Verzeichnisserver können bei einer Überschreitung des Grenzwerts für falsche Kennwörter oder durch Administratoraktionen gesperrt werden.

Vorgehensweise

Falls Sie ein gesperrtes Kennwort nicht entsperren können, führen Sie die folgenden Schritte aus:

1. Geben Sie das Kennwort an den Server zurück, indem Sie den folgenden Befehl (Beispiel) ausführen:
   `update node node_x Neues Kennwort authentication=local`
2. Bereinigen Sie den LDAP-Verzeichnisserver, indem Sie den folgenden Befehl (Beispiel) ausführen:
   `audit ldapdirectory fix=yes wait=no`

Dieser Befehl entfernt Knoten und Administrator-IDs, die auf dem LDAP-Verzeichnisserver gespeichert sind und die Kennwörter nicht mit einem LDAP-Verzeichnisserver authentifizieren.

3. Melden Sie sich beim Knoten ab.
4. Geben Sie den folgenden Befehl aus:

   ```
   update node Neuestes Kennwort für Knoten X authentication=ldap
   ```

5. Melden Sie sich mit dem neuen Kennwort beim Knoten an.

LDAP-Verzeichnisserver zur Bereinigung des Servers prüfen

Wenn der LDAP-Verzeichnisserver mit dem -Server synchron ist, erleichtert dies Ihre Arbeit. Ein LDAP-Verzeichnisserver enthält möglicherweise Hunderte von Einträgen, die nicht mehr verwendet werden. Außerdem könnte es sein, dass bestimmte Administrator- oder Knoteneinträge entgegen Ihrer Vermutung nicht auf dem LDAP-Verzeichnisserver vorhanden sind.

Durch eine Prüfung können Sie feststellen, bei welchen Einträgen für Administrator-IDs oder Knoten die Authentifizierung der Kennwörter mit dem LDAP-Verzeichnisserver definiert ist. Sie können den LDAP-Verzeichnisserver prüfen, um nicht verwendete Kennwörter, Administratoren und Knoten zu löschen. Es kann vorkommen, dass der von IBM Spectrum Protect gesteuerte Namensbereich auf dem LDAP-Verzeichnisserver nicht mehr mit den gespeicherten Daten auf dem IBM Spectrum Protect-Server synchron ist.

Falls der Administrator des LDAP-Verzeichnisservers Einträge des externen Verzeichnisses manuell geändert hat, sind diese Einträge nicht synchron. Auch der IBM Spectrum Protect-Server kann die Synchronität mit dem LDAP-Server verlieren, wenn Sie den Standardbefehl **SYNCLDAPDELETE=NO** bei einem Befehl **REMOVE**, **RENAME** oder **UPDATE** verwenden. Der Befehl **AUDIT LDAPDIRECTORY** löscht alle Einträge aus dem LDAP-Verzeichnisserver, die nicht mit der IBM Spectrum Protect-Datenbank korrelieren. Außerdem gibt der Befehl Warnungen aus, die Ihnen bei der Korrektur von Einträgen helfen.

Warnungen werden ausgegeben, wenn Kennwörter, die mit dem LDAP-Verzeichnisserver authentifiziert werden, in der IBM Spectrum Protect-Datenbank, aber nicht im LDAP-Namensbereich gespeichert sind. Ausgehend von den Warnungen können Sie das Problem mit dem Befehl **UPDATE NODE** oder **UPDATE ADMIN** korrigieren.

Beispiel: LDAP-Verzeichnisserver prüfen

Falls der IBM Spectrum Protect-Namensbereich auf dem LDAP-Verzeichnisserver nicht mit der IBM Spectrum Protect-Datenbank synchron ist, geben Sie den folgenden Befehl aus:

```
AUDIT LDAPDIRECTORY FIX=YES
```

Der Befehl erzeugt eine Liste aller Knoten und Administratoren, die aus dem LDAP-Verzeichnisserver entfernt wurden. Er erstellt außerdem eine Liste aller Knoten und Administratoren, die auf dem LDAP-Verzeichnisserver fehlen. Wenn Sie ermitteln wollen, welche Einträge nicht synchron sind, verwenden Sie die Standardeinstellung **FIX=NO**, damit Abweichungen zwischen den Servern gemeldet werden.

Anmerkung: Verwenden Sie nicht die Einstellung **FIX=YES**, falls mehrere IBM Spectrum Protect-Server den Namensbereich für das LDAP-Verzeichnis gemeinsam

nutzen.

Fehlernachrichten für mit LDAP authentifizierte Kennwörter

Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, können bei der Verbindung zwischen dem -Server und dem LDAP-Verzeichnisserver allgemeine Fehler auftreten.

Die folgenden Fehlernachrichten sind das Ergebnis der Kommunikation mit einem LDAP-Verzeichnisserver:

ANR3114E

Die Nachricht ANR3114E wird immer dann ausgegeben, wenn während einer LDAP-Operation ein unerwarteter Fehler auftritt. Die Nachricht enthält weitere Informationen, die bei der Behebung des Fehlers hilfreich sind. Beispiel:

```
ANR3114E LDAP-Fehler
LDAP-Fehlercode (Fehlerbeschreibung) bei Operation.
```

LDAP-Fehlercode

Die Fehlernummer, die entweder von der LDAP-Clientschnittstelle oder vom LDAP-Verzeichnisserver zurückgegeben wurde.

Fehlerbeschreibung

Eine Beschreibung des *LDAP-Fehlercodes*, in der die Fehlerursache angegeben ist.

Operation

Die LDAP-Clientoperation, die ausgeführt wurde, als der Fehler auftrat.

Im folgenden Beispiel wird der Fehlercode 53 von der LDAP-Clientschnittstelle oder vom LDAP-Verzeichnisserver zurückgegeben. Die Operation, die beim Auftreten des Fehlers ausgeführt wurde, ist ebenfalls angegeben. In diesem Beispiel heißt die Operation 'ldap_search_s'.

```
ANR3114E
LDAP-Fehler 53 (DSA wird nicht ausgeführt) bei ldap_search_s.
```

ANR3115E

Die Nachricht ANR3115E wird bei einem Fehler für den LDAP-Verzeichnisserver ausgegeben. Beispiel:

```
ANR3115E Der LDAP-Verzeichnisserver hat die folgende Fehlernachricht
(LDAP-Servernachricht) mit dem LDAP-Fehler zurückgegeben.
```

LDAP-Servernachricht

Dieser Nachrichtentext wurde vom LDAP-Verzeichnisserver zurückgegeben und enthält weitere Informationen zu dem soeben aufgetretenen Fehler.

ANR3116E

Die Fehlernachricht ANR3116E wird ausgegeben, wenn die Komponente 'Global Security ToolKit' (GSKit) während einer LDAP-Operation einen Fehler feststellt. GSKit stellt Secure Sockets Layer/Transport Layer Security (SSL/TLS) für LDAP-Operationen bereit. Diese Fehlernachricht hängt normalerweise mit SSL/TLS, Zertifikaten, der Verschlüsselung oder mit Netzoperationen zusammen. Beispiel:

```
ANR3116E LDAP-SSL/TLS-Fehler GSKIT-Fehlercode (Fehlerbeschreibung)
während Operation aufgetreten.
```

GSKit-Fehlercode
Die von der Komponente GSKit zurückgegebene Fehlernummer.

Fehlerbeschreibung
Eine Textbeschreibung, die dem *Fehlercode* zugeordnet ist und die Fehlerursache angibt.

Operation
Die LDAP-Clientoperation, die ausgeführt wurde, als der Fehler auftrat.

Falls Sie die Ursache der Fehler nicht ermitteln können, führen Sie die folgenden Schritte aus:

1. Untersuchen Sie die Servernachrichten, die etwa zu derselben Zeit wie die Fehlernachricht ausgegeben wurden, um die Ursache und die Auswirkung des Fehlers zu bestimmen. Geben Sie den Befehl **QUERY ACTLOG** aus, um die Aktivitätenprotokolldatei anzuzeigen und in dieser Datei nach Fehlernachrichten zu suchen.
2. Stellen Sie fest, ob Netzprobleme vorliegen.
3. Überprüfen Sie den Status des LDAP-Verzeichnisservers.
4. Suchen Sie bei der Fehlernachricht ANR3116E nach Problemen in Bezug auf die vom LDAP-Verzeichnisserver verwendeten Zertifikate oder im Zusammenhang mit der Schlüsseldatenbank des IBM Spectrum Protect-Servers (`cert.kdb`).
5. Untersuchen Sie die Protokolldateien des LDAP-Verzeichnisservers.
6. Grenzen Sie das Problem mithilfe von LDAP-Dienstprogrammen wie 'ldapsearch' oder 'ldp' ein.

Die folgende Tabelle enthält Fehler, die auftreten können, falls die Konfiguration nicht korrekt ist.

Tabelle 1. Mögliche Fehler bei der Authentifizierung von Kennwörtern mit einem LDAP-Verzeichnisserver

Fehlernachrichten	Lösung
ANR3114E LDAP-Fehler 118 (SSL-Bibliothek kann nicht geladen werden) ANR3116E LDAP-SSL/TLS-Fehler 118 (Unbekannter SSL-Fehler) ANR3103E Bei der Initialisierung der LDAP-Verzeichnisservices ist ein Fehler aufgetreten	Möglicherweise ist der Bibliothekspfad nicht ordnungsgemäß definiert. Stellen Sie sicher, dass Sie die richtige Version von GSKit verwenden.
ANR3114E LDAP-Fehler 116 (Zum SSL-Server konnte keine Verbindung hergestellt werden) ANR3116E LDAP-SSL/TLS-Fehler 406 (E/A-Fehler) ANR3103E Bei der Initialisierung der LDAP-Verzeichnisservices ist ein Fehler aufgetreten ANR2732E Kommunikation mit dem externen LDAP-Verzeichnisserver nicht möglich	Möglicherweise wird von Directory Server nicht die richtige GSKit-Version verwendet. Führen Sie ein Upgrade auf die richtige GSKit-Version durch. Siehe Technote 1469388. Inaktivieren Sie für Active Directory die automatischen Aktualisierungen des Stammzertifikats mit einem Windows-Update, falls keine Internetverbindung verfügbar ist.

Tabelle 1. Mögliche Fehler bei der Authentifizierung von Kennwörtern mit einem LDAP-Verzeichnisserver (Forts.)

Fehlernachrichten	Lösung
ANR3114E LDAP-Fehler 52 (DSA ist nicht verfügbar) ANR3103E Bei der Initialisierung der LDAP-Verzeichnisservices ist ein Fehler aufgetreten ANR2732E Kommunikation mit dem externen LDAP-Verzeichnisserver nicht möglich	Der Active Directory-Server verfügt nicht über ein Zertifikat für TLS/SSL. Erstellen Sie ein signiertes Zertifikat, das von Microsoft Active Directory verwendet werden kann.
ANR3114E LDAP-Fehler 116 (Zum SSL-Server konnte keine Verbindung hergestellt werden) ANR3116E LDAP-SSL/TLS-Fehler 414 (Falsches Zertifikat) ANR3103E Bei der Initialisierung der LDAP-Verzeichnisservices ist ein Fehler aufgetreten ANR2732E Kommunikation mit dem externen LDAP-Verzeichnisserver nicht möglich	Das Zertifikat des LDAP-Verzeichnisservers ist nicht vertrauenswürdig. Fügen Sie das Zertifikat der Rootzertifizierungsstelle zur Schlüsseldatenbankdatei des IBM Spectrum Protect-Servers (`cert.kdb`) hinzu und stellen Sie sicher, dass die Zertifikate nicht abgelaufen sind.
ANR3094E Der definierte Name (DN), der in der Option **LDAPURL** angegeben wurde, ist auf dem LDAP-Verzeichnisserver nicht vorhanden ANR3103E Bei der Initialisierung der LDAP-Verzeichnisservices ist ein Fehler aufgetreten	Falls der definierte Name (DN) vorhanden ist, besitzt der Benutzer **LDAPUSER** möglicherweise keine Steuerungsberechtigung für den uneingeschränkten Zugriff auf den Basis-DN, der in der Option **LDAPURL** definiert ist.
ANR3114E LDAP-Fehler 50 (Unzureichender Zugriff) ANR1885E Initialisierung des LDAP-Verzeichnisservice: Die Berechtigung wurde verweigert, als auf den LDAP-Verzeichniseintrag als LDAPUSER zugegriffen wurde ANR3103E Bei der Initialisierung der LDAP-Verzeichnisservices ist ein Fehler aufgetreten ANR1885E SET LDAPPASSWORD: Die Berechtigung wurde verweigert, als auf den **LDAPUSER**-Eintrag zugegriffen wurde	Der Benutzer **LDAPUSER** besitzt keine Steuerungsberechtigungen für den uneingeschränkten Zugriff auf den Basis-DN, der in der Option **LDAPURL** definiert ist.
ANR3114E LDAP-Fehler 116 (Zum SSL-Server konnte keine Verbindung hergestellt werden) ANR3116E LDAP-SSL/TLS-Fehler 420 (Socket geschlossen)	Für Directory Server ist die Option SSL_TIMEOUT_MILLISEC mit einem Wert definiert, der nicht groß genug ist. Siehe Technote 1233758.
ANR3114E LDAP-Fehler 4 (Größenbeschränkung überschritten)	Setzen Sie die Suchgrößenbeschränkung für den LDAP-Server herauf, damit die Gesamtzahl der mit LDAP authentifizierten Knoten und Administratoren berücksichtigt wird.

Tabelle 1. Mögliche Fehler bei der Authentifizierung von Kennwörtern mit einem LDAP-Verzeichnisserver (Forts.)

Fehlernachrichten	Lösung
ANR3114E LDAP-Fehler 91 (Verbindungsfehler) bei ldap_sasl_bind. ANR3103E Bei der Initialisierung der LDAP-Verzeichnisservices ist ein Fehler aufgetreten.	Der LDAP-Server ist offline oder nicht aktiv.

Fehler für Clientzeitplanung beheben

Der Administrator für IBM Spectrum Protect kann die automatische Ausführung von Tasks planen.

Wenn Sie Probleme mit Ihrem Client-Scheduler feststellen, können Sie die folgenden Diagnoseschritte verwenden, um die Fehlerursache zu bestimmen:

- Hinzufügungen und Änderungen an den Clientoptionen werden vom Client-Scheduler erst nach dem nächsten geplanten Start erkannt. Löschungen in der Clientoptionsgruppe werden erst wirksam, nachdem der Scheduler erneut gestartet wurde.
- Hinzufügungen, Löschungen und Änderungen an Zeitplänen, die vom Client-Akzeptor verwaltet werden, werden beim nächsten geplanten Start erkannt.
- Verwenden Sie das Diagnosetool **SHOW PENDING**, um Zeitpläne, Knoten und die nächste geplante Ausführungszeit anzuzeigen.
- Überprüfen Sie in der Clientoptionsdatei die `dsm.sys`-Zeilengruppe für den Knoten und die Werte der Optionen `MANAGEDSERVICES`, `PRESCHEDCMD` und `POSTSCHEDCMD` auf Informationen, nachdem ein Knoten ein geplantes Ereignis versäumt hat.

Status eines geplanten Ereignisses bestimmen

Der Server verwaltet einen Datensatz aller geplanten Ereignisse. Die Datensätze sind hilfreich, um IBM Spectrum Protect-Zeitpläne auf zahlreichen Client-Computern verwalten zu können.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Ereignisdatensätze auf einem Server anzuzeigen:

Vorgehensweise

1. Geben Sie den Befehl **QUERY EVENT** aus.
2. Geben Sie die folgende Abfrage aus, um alle Ereignisergebnisse des vorherigen Tags anzuzeigen:

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

3. Geben Sie die folgende Abfrage aus, um die Abfrageergebnisse auf Ausnahmefälle zu begrenzen:

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

Nächste Schritte

Die Abfrageergebnisse umfassen ein Statusfeld, das eine Zusammenfassung des Ergebnisses für ein bestimmtes Ereignis liefert. Wenn die Option `format=detailed` verwendet wird, können Sie auch das Ergebnis eines Ereignisses anzeigen, bei dem es sich um den Gesamtrückkehrcode handelt, der vom Client zurückgegeben wird. Informationen zu geplanten und abgeschlossenen Ereignissen finden Sie unter dem Befehl **QUERY EVENT**.

Serveraktivitätenprotokoll auf Fehler überprüfen

Wenn ein geplantes Ereignis versäumt wird, aber andere aufeinanderfolgende geplante Ereignisse für diesen Knoten das Ergebnis `Abgeschlossen` zeigen, überprüfen Sie das Serveraktivitätenprotokoll und das Clientzeitplanprotokoll auf Fehler.

Wenn Sie das Serveraktivitätenprotokoll überprüfen, grenzen Sie die Abfrageergebnisse auf den Zeitraum um das geplante Ereignis herum ein. Beginnen Sie die Ereignisprotokollabfrage zu einem Zeitpunkt, der kurz vor dem Startfenster des betreffenden geplanten Ereignisses liegt. Untersuchen Sie beispielsweise das folgende verdächtige Ereignis:

```
Geplanter Start      Ist-Start            Zeitplanname  Knotenname    Status
-------------------- -------------------- ------------- ------------- -------
08/21/2003 08:27:33 HOURLY NODEA Missed
```

Anschließend können Sie eine der folgenden Abfragen ausgeben:

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

Der Client speichert ein ausführliches Protokoll aller geplanten Aktivitäten. Überprüfen Sie das lokale Planungsprotokoll des Clients, wenn Abfragen des Serveraktivitätenprotokolls keine Erklärungen für ein fehlgeschlagenes geplantes Ereignis bereitstellen.

Sie benötigen Zugriff auf den Client-Computer, um die Planungsprotokolldatei untersuchen zu können. Das Planungsprotokoll wird normalerweise in der Datei `dsmsched.log` und in demselben Verzeichnis wie die Datei `dsmerror.log` gespeichert. Die Position der Protokolldatei kann mit Clientoptionen angegeben werden. Sie müssen daher möglicherweise anhand der Optionsdatei ermitteln, ob die Protokolldatei mit der Option `SCHEDLOGNAME` verlagert wurde. Unter Windows kann das Planungsprotokoll auch mit einer Optionseinstellung verlagert werden, die Teil der Zeitplanungsservicedefinition ist. Sie können mit dem Befehl **DSMCUTIL QUERY** überprüfen, ob diese Option definiert wurde. Wenn Sie das Planungsprotokoll lokalisiert haben, suchen Sie in der Datei nach dem Zeitraum, der dem Startdatum und der Startzeit des betreffenden geplanten Ereignisses entspricht. Die folgende Liste enthält allgemeine Suchparameter:

- Wenn Sie ein versäumtes Ereignis untersuchen, überprüfen Sie die Details des vorherigen Ereignisses, einschließlich der Zeit, zu der das vorherige Ereignis beendet wurde.
- Wenn Sie ein fehlgeschlagenes Ereignis untersuchen, suchen Sie nach Fehlernachrichten, die den Fehler erklären (z. B. Grenzwert für Serversitzung, der überschritten wurde).
- Ist die Erläuterung noch immer nicht klar, müssen Sie die Fehlerprotokolldatei des Clients überprüfen (normalerweise `dsmerror.log`).

Client-Service starten und stoppen

Das Starten und Stoppen des Client-Service kann manchmal zur Behebung von Problemen mit der Clientzeitplanung beitragen.

Tipp: Wenn Sie viele Clients verwalten, auf denen Schedulerprozesse ausgeführt werden, kann es sinnvoll sein, auch den Client-Service von einem fernen Computer aus starten und stoppen zu können. Der Client für Windows stellt ein Dienstprogramm zur Unterstützung der Fernverwaltung des Scheduler-Service bereit. Für andere Betriebssysteme sind standardmäßige Betriebssystemdienstprogramme erforderlich.

Windows Um den Client-Scheduler-Service über Fernzugriff mit dem Befehl **DSMCUTIL** und der Option `/computer:` zu verwalten, müssen Sie über Administratorrechte in der Domäne des Zielcomputers verfügen. Um zu bestimmen, ob der Scheduler-Service auf einem fernen Computer ausgeführt wird, überprüfen Sie in einer Abfrage, die der folgenden Abfrage ähnelt, das Feld **Aktueller Status**:

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

Geben Sie die folgenden Abfragen aus, um einen Scheduler-Service erneut zu starten, für den keine Zeitpläne vorhanden sind:

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

Wenn Sie den Clientakzeptordämon (CAD) zur Verwaltung des Schedulers verwenden, müssen Sie daher möglicherweise den CAD-Service erneut starten oder den Scheduler-Service stoppen und den CAD-Service erneut starten, indem Sie die folgenden Abfragen ausgeben:

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

AIX Linux Wenn Sie den Scheduler mit dem konventionellen Verfahren verwalten, können Sie ein Shell-Script schreiben, um nach IBM Spectrum Protect-Schedulern oder Clientakzeptorprozessen zu suchen und deren Ausführung zu stoppen, und dann die Prozesse erneut starten. Das folgende Beispiel-Shell-Script zeigt, wie der IBM Spectrum Protect-Schedulerprozess gestoppt und erneut gestartet wird:

```
#!/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 Falls Sie den Client-Scheduler mit dem Clientakzeptordämon verwalten wollen, legen Sie für die Option `managedservices` die Einstellung **`schedule`** oder **`schedule webclient`** in der Datei `dsm.sys` fest. Falls Sie bei Mac OS X die Option `managedservices` nicht angeben, verwaltet der Clientakzeptordämon standardmäßig sowohl den Scheduler als auch den Web-Client.

AIX Fügen Sie den folgenden Eintrag in die Systemstartdatei ein (diese Datei heißt bei den meisten Plattformen `/etc/inittab`):

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

Linux Das Installationsprogramm des Clients für Sichern/Archivieren erstellt ein Startscript für den Clientakzeptordämon (**`dsmcad`**) im Verzeichnis `/etc/init.d`. Sie können den Clientakzeptordämon mit dem Standardbefehl **`service`** unter Linux starten, stoppen, erneut starten und abfragen. Beispiel:

```
# service dsmcad start
# service dsmcad stop
# service dsmcad restart
# service dsmcad statis
```

Um das automatische Starten des Clientakzeptordämons nach einem Systemwiederanlauf zu ermöglichen, fügen Sie den Service folgendermaßen über eine Shelleingabeaufforderung hinzu:

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

Mac OS X Sie können den Clientakzeptordämon mit dem Dienstprogramm **`launchd`** starten oder stoppen. Geben Sie zum Starten des Clientakzeptordämons den folgenden Befehl im **Terminalfenster** aus:

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

Geben Sie zum Stoppen des Clientakzeptordämons den folgenden Befehl im **Terminalfenster** aus:

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

Zur Steuerung des Clientakzeptordämons können Sie auch die Anwendung **TSM-Tools für Administratoren** verwenden.

Fehler beim Einschließen oder Ausschließen von Clientdateien während der Sicherungsverarbeitung beheben

Die Einschluss/Ausschlussverarbeitungsoption hat Auswirkungen darauf, welche Dateien für eine Sicherungs- oder Archivierungsoperation an den Server gesendet werden. Es sind mehrere mögliche Ursachen vorhanden, wenn Sie implizit oder explizit angeben, dass eine Datei während der Sicherungsverarbeitung eingeschlossen oder ausgeschlossen werden soll, aber die Datei nicht korrekt verarbeitet wird.

Durch die Clientoptionsgruppe auf dem Server ein- oder ausgeschlossene Dateien identifizieren

Der IBM Spectrum Protect-Administrator kann Dateien im Namen des Clients einschließen oder ausschließen. INCLUDE- oder EXCLUDE-Anweisungen, die vom Server stammen, setzen INCLUDE- und EXCLUDE-Anweisungen außer Kraft, die in die lokale Clientoptionsdatei eingegeben werden.

Wenden Sie sich an den IBM Spectrum Protect-Serveradministrator, um das Problem zu lösen.

Sie können den Befehl **DSMC QUERY INCLEXCL** des Clients für Sichern/Archivieren ausgeben, um die Dateien zu identifizieren, die durch die Clientoptionsgruppe auf dem Server ein- oder ausgeschlossen sind. In der Ausgabe dieses Befehls erscheint „Operating System" als Quellendatei für Dateien, die automatisch von der Sicherungsverarbeitung ausgeschlossen wurden. In diesem Beispiel geben die Benutzer an, dass alle Dateien mit der Dateinamenerweiterung „.o" in die lokale Optionsdatei aufgenommen werden sollen, der Server sendet dem Client jedoch eine Option, die alle Dateien mit der Dateinamenerweiterung „.o" ausschließt. Die vom Server angegebene Option hat Vorrang.

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

Optionen, die vom Server an den Client übergeben werden, werden in Gruppen bereitgestellt. Das heißt, alle INCLUDE-Optionen werden in einer Gruppe gesendet und alle EXCLUDE-Optionen werden in einer Gruppe gesendet, wenn die Optionen INCLUDE und EXCLUDE auf dem Server unterstützt werden. Sie können diese Optionen nicht mischen, um ein gewünschtes Ergebnis zu erzielen, bei dem einige Dateien in ausgeschlossenen Verzeichnissen eingeschlossen werden. Mithilfe der Option INCLEXCL können Sie die Optionen INCLUDE und EXCLUDE mischen und sortieren.

Dateien automatisch von der Sicherungsverarbeitung ausschließen

Bestimmte Dateien werden von der Sicherungsanwendung nicht gesichert, da sie für die Sicherung nicht benötigt werden oder die Dateien von IBM Spectrum Protect für die interne Verarbeitung verwendet werden.

Wenn bestimmte Dateien bei der Sicherungsverarbeitung berücksichtigt werden müssen, können sie von IBM Spectrum Protect durch Einfügen von *INCLUDE*-Anweisungen in die auf dem Server definierten Clientoptionen einbezogen werden.

Wichtig: Da einige Dateien explizit als nicht zu sichernde Dateien angegeben wurden, sollten Sie sie nicht in die Clientoptionsgruppe auf dem Server aufnehmen.

Geben Sie den Befehl **DSMC QUERY INCLEXCL** des Clients für Sichern/Archivieren aus, um die Dateien zu identifizieren, die nicht gesichert wurden. In der Ausgabe des Befehls **DSMC QUERY INCLEXCL** erscheint „Operating System" als Quellendatei für Dateien, die automatisch von der Sicherungsverarbeitung ausgeschlossen wurden.

Windows Beispielsweise wird die folgende Ausgabe angezeigt, wenn Sie den Befehl **DSMC QUERY INCLEXCL** ausgegeben haben:

```
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
```

Tabelle 2 enthält die Dateien, die automatisch ausgeschlossen werden.

Tabelle 2. Während der Sicherungsverarbeitung automatisch ausgeschlossene Dateien

Plattform	Ausgeschlossene Dateien

Windows	• Im Registrierungsschlüssel `HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup` aufgelistete Dateien
	• Das Clientverzeichnis zur Zwischenspeicherung `C:\ADSM.SYS`
	• IIS-Metadateien (IIS = Internet Information Server) (diese Dateien werden in der Systemobjekt- oder Systemstatussicherung verarbeitet)
	• Registry-Dateien (diese Dateien werden in der Systemobjekt- oder Systemstatussicherung verarbeitet)
	• Client-Tracedateien
	• Systemdateien
	Windows-Systemdateien werden automatisch von der Sicherungsverarbeitung des Systemlaufwerks ausgeschlossen und können nicht eingeschlossen werden.
	Damit diese Windows-Systemdateien verarbeitet werden, müssen Sie einen Befehl **DSMC BACKUP SYSTEMSTATE** ausgeben.
	Die Windows-Systemdateien werden von der Sicherungsverarbeitung des Systemlaufwerks ausgeschlossen, weil sie während der Systemobjekt- oder Systemstatussicherung gesendet werden. Systemdateien sind Bootdateien, Katalogdateien, Leistungsdatendateien und durch den Windows-Systemdateischutz (System File Protection, SFP) geschützte Dateien. Diese Dateien werden während der Sicherung des Systemlaufwerks nicht verarbeitet. Die Dateien sind jedoch intern von der Verarbeitung des Systemlaufwerks ausgeschlossen und nicht explizit durch Exclude-Anweisungen, da zu viele Exclude-Anweisungen erforderlich wären, um alle diese Dateien anzugeben. Die Leistung bei der Sicherung kann beeinträchtigt werden.
	Sie können den Befehl **DSMC QUERY SYSTEMINFO** des Clients für Sichern/Archivieren ausgeben, um die Windows-Systemdateien zu identifizieren. Die Ausgabe dieses Befehls wird in die Datei `dsminfo.txt` geschrieben.
	`(Auszug aus der Datei dsmfino.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`

AIX Linux	Client-Tracedateien
Mac OS X	• Vom Betriebssystem verwendete nicht permanente Dateien, temporäre Dateien und Einheitendateien • Client-Tracedateien

Dateien mit der Anweisung EXCLUDE.DIR ausschließen

Die Anweisung EXCLUDE.DIR schließt alle Verzeichnisse und Dateien unter dem übergeordneten Verzeichnis aus.

Sollen alle Dateien, die mit einem Dateimuster übereinstimmen, unabhängig von ihrer Position in einer Verzeichnisstruktur eingeschlossen werden, verwenden Sie keine EXCLUDE.DIR-Anweisungen.

Betrachten Sie z. B. die folgenden Anweisungen include und exclude: AIX Linux Mac OS X

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

Windows

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

Die Anweisung INCLUDE in diesem Beispiel gibt an, dass alle Dateien mit der Erweiterung .o eingeschlossen werden sollen. Durch die vorangehende Anweisung EXCLUDE.DIR werden jedoch alle Dateien im Verzeichnis /usr ausgeschlossen, auch wenn sie die Erweiterung .o haben. Die Reihenfolge der beiden Anweisungen spielt hierbei keine Rolle.

Wenn Sie alle Dateien mit der Erweiterung .o sichern wollen, verwenden Sie folgende Syntax: AIX Linux Mac OS X

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

Windows

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

Wenn Sie in Einschluss-/Ausschlussanweisungen Platzhalterzeichen einsetzen wollen, verwenden Sie zum Ein- bzw. Ausschließen aller Dateien das Zeichen * und nicht das Muster *.*.*.*. Das Muster *.*.*.* bedeutet, dass alle Dateien ein- bzw. ausgeschlossen werden sollen, die mindestens einen Punkt (.) enthalten, während das Zeichen * angibt, dass alle Dateien ein- bzw. ausgeschlossen werden. Wenn Sie *.* verwenden, werden Dateien, deren Namen keine Punkte enthalten (z. B. C:\MYDIR\MYFILE unter Windows), nicht gefiltert.

Wenn Sie eine selektive Sicherung oder eine partielle Teilsicherung einer einzelnen Datei über den Befehlszeilenclient ausführen wollen, wirkt sich die Option EXCLUDE.DIR nicht auf sie aus.

Wenn Sie eine selektive Sicherung oder eine partielle Teilsicherung einer einzelnen Datei über den Befehlszeilenclient starten, wird die Datei auch dann verarbeitet, wenn eine Anweisung EXCLUDE.DIR vorhanden ist, die eines der übergeordneten Verzeichnisse im Dateipfad ausschließt.

Beispiel: Die folgende include/exclude-Anweisung wird in nachfolgenden Befehlszeilenaktionen verwendet: AIX Linux Mac OS X

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

Windows

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

Die folgende selektive Sicherung führt immer zu einer Verarbeitung der Datei:

AIX Linux Mac OS X

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

Windows

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

Wenn Sie eine selektive Sicherung ausgeben, die ein Platzhalterzeichen enthält, werden keine Dateien verarbeitet, weil das Verzeichnis ausgeschlossen ist: AIX Linux Mac OS X

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

Windows

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

Wichtig: Bei einer nachfolgenden Teilsicherung des Dateisystems `/home` wird die Datei `/home/spike/my.file` inaktiviert. Analog wird unter Windows bei einer nachfolgenden Teilsicherung des Verzeichnisses `C:\Users` die Datei `C:\Users\spike\my.file` inaktiviert.

Beenden Sie Anweisungen `EXCLUDE.DIR` nicht mit einem Verzeichnisbegrenzer.

Die folgenden Beispiele zeigen `EXCLUDE.DIR`-Anweisungen, die aufgrund eines Verzeichnisbegrenzer am Ende des Verzeichnispfads nicht korrekt sind: AIX Linux

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

Mac OS X

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

Windows

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

Die folgenden Beispiele zeigen die korrekte Angabe von `EXCLUDE.DIR`: AIX Linux

```
exclude.dir /usr
```

Mac OS X

```
exclude.dir /Users
```

Windows

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

Ein- oder Ausschluss von Dateien mit Anweisungen für Komprimierung, Verschlüsselung und Subdateisicherung bestimmen

Einschluss- und Ausschlussanweisungen für Komprimierung (INCLUDE.COMPRESS), Verschlüsselung (INCLUDE.ENCRYPT) und Subdateisicherung (INCLUDE.SUBFILE) implizieren nicht, dass die Datei bei der Sicherungsverarbeitung berücksichtigt wird.

Sie können die Anweisungen INCLUDE und EXCLUDE zusammen mit den Anweisungen COMPRESS, ENCRYPT und SUBFILE verwenden, um die gewünschten Ergebnisse zu erhalten.

Betrachten Sie das folgende Beispiel: AIX Linux Mac OS X

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

Windows

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

Diese Anweisung gibt an, dass die Datei `/usr/file.o` von der Sicherungsverarbeitung ausgeschlossen wird. Die Anweisung INCLUDE.COMPRESS gibt Folgendes an: Wenn eine Datei ein Kandidat für die Sicherungsverarbeitung ist und dem Muster `/usr/*.o` entspricht, ist die Datei zu komprimieren. Die Anweisung INCLUDE.COMPRESS darf nicht wie folgt interpretiert werden: Alle Dateien, die mit dem Muster `/usr/*.o` übereinstimmen, sind zu sichern und zu komprimieren. Wenn die Datei `/usr/file.o` in diesem Beispiel gesichert werden soll, müssen Sie die Anweisung EXCLUDE entfernen.

Begrenzer zum Einschließen oder Ausschließen von Dateien verwenden

Wenn die Datenträgerbegrenzer oder Verzeichnisbegrenzer nicht korrekt sind, kann dies zur Folge haben, dass die Anweisungen `INCLUDE` und `EXCLUDE` nicht korrekt arbeiten.

Eine plattformspezifische Anweisung `INCLUDE` oder `EXCLUDE` enthält Syntax für „alles" und „alle Dateien unter einem bestimmten Verzeichnis".

Wenn Sie eine Anweisung `INCLUDE` für „alle Dateien unter einem bestimmten Verzeichnis" verwenden möchten, stellen Sie sicher, dass die Schrägstriche und Datenträgerbegrenzer korrekt sind. Orientieren Sie sich an den folgenden Beispielen, wenn alle Dateien unter dem Verzeichnis „home" eingeschlossen werden sollen:

Windows **Verwendung des umgekehrten Schrägstrichs "\" und des Datenträgerbegrenzers ":"**

```
*include alles im Verzeichnis c:\home
include c:\home\...\*
*include alles
include *:\...\*
```

AIX Linux Mac OS X **Verwendung des Schrägstrichs "/"**

```
*include alles im Verzeichnis /home
include /home/.../*
*include alles
include /.../*
```

Fehler durch eine nicht ordnungsgemäß codierte Einschluss- oder Ausschlussliste beheben

Aufgrund der Komplexität oder der Anzahl von INCLUDE- und EXCLUDE-Anweisungen kann es zu einem nicht beabsichtigten Einschluss bzw. Ausschluss einer Datei kommen.

Konfigurieren Sie den Client mit der Tracemarkierung **INCLEXCL**, damit Sie einfacher feststellen können, warum eine Datei ein- bzw. ausgeschlossen wurde.

Sie glauben beispielsweise, dass die Datei `c:\home\file.txt` bei der Sicherungsverarbeitung berücksichtigt werden sollte. Der Trace zeigt, dass es eine Anweisung EXCLUDE gibt, die diese Datei ausschließt:

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

Der Befehl **DSMC QUERY INCLEXCL** des Clients für Sichern/Archivieren zeigt, dass sich diese Anweisung in der Clientoptionsgruppe auf IBM Spectrum Protect-Server befindet:

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

Momentaufnahmedifferenzprobleme beheben

AIX Linux Windows

Sie können Teilsicherungen von N-Series- und NetApp-Dateiserverdatenträgern schneller ausführen, wenn Sie die NetApp-Momentaufnahmedifferenz-API verwenden.

Voraussetzungen

Um die Momentaufnahmedifferenzfunktion zu verwenden, müssen Sie zuerst eine NetApp-Benutzer-ID und ein Kennwort auf dem Client definieren. Die Benutzer-ID und das Kennwort sind für IBM Spectrum Protect erforderlich, um die Verbindung zum Dateiserver herzustellen. Definieren Sie bei AIX und Linux eine Benutzer-ID und ein Kennwort mit Rootberechtigung oder bei Windows eine Benutzer-ID und ein Kennwort mit Administratorberechtigung. Setzen Sie die Berechtigungsstufe auf die Berechtigungsstufe, die verwendet wird, wenn der Dateiserverdatenträger zugeordnet oder bereitgestellt wird. Stellen Sie sicher, dass der vollständig qualifizierte Hostname oder die IP-Adresse in Schreibweise mit Trennzeichen für den Dateiservernamen verwendet wird. Geben Sie den Befehl **SET PASSWORD** des Clients für Sichern/Archivieren aus, um diese Informationen mit der Benutzer-ID und dem Kennwort zu speichern.

Hinweis: Der Befehl **DSMC SET PASSWORD** wurde erweitert, um Kennwörter des Typs „Dateiserver" zu speichern.

Die Momentaufnahmedifferenzfunktion vergleicht zwei Momentaufnahmen (Basis und Differenz) und gibt für die beiden Momentaufnahmen eine Liste der Dateien zurück, die geändert, gelöscht oder hinzugefügt wurden. IBM Spectrum Protect sichert diese Dateiliste, anstatt das Dateisystem nach Änderungen zu durchsuchen.

Die Momentaufnahmedifferenzfunktion unterstützt die folgenden Features, die nur auf der Datenträgerebene gültig sind:

- NetApp-/N-Series-Dateiserver, auf denen Data ONTAP Release 7.3 oder höher ausgeführt wird
- Windows Über Common Internet File System (CIFS) angeschlossene Datenträger
- Konventionelle Dateiserverdatenträger und FlexVol-Dateiserverdatenträger
- Java- und Web-Client-GUI
- AIX Linux Über Network File System (NFS) angeschlossene Datenträger

Die Momentaufnahmedifferenzfunktion unterstützt nicht die folgenden Features:

- An ein SAN angeschlossene NetApp-/N-Series-Datenträger
- QTrees oder Unterverzeichnisse
- vFiler-Datenträger mit einem Dateiserver, auf dem ONTAP Version 8.1.0 oder früher ausgeführt wird, werden nicht unterstützt. vFiler-Datenträger mit einem Dateiserver, auf dem ONTAP Version 8.1.1 oder höher ausgeführt wird, werden unterstützt.

Windows

Typ des Dateiserverdatenträgers überprüfen

IBM Spectrum Protect erwartet NTFS (New Technology File System) als CIFS-Sicherheitstyp (CIFS = Common Internet File System). Verwenden Sie NetApp FilerView und stellen Sie sicher, dass der CIFS-Sicherheitstyp auf „ntfs" gesetzt ist.

Einschränkungen für Momentaufnahmedifferenz

Die fehlende Unicode-Unterstützung in NetApp verhindert, dass IBM Spectrum Protect Dateien verarbeitet, die Zeichen verwenden, die sich nicht im 7-Bit-ASCII-Bereich befinden. IBM Spectrum Protect kann nur Namen sichern, die ASCII-Zeichen enthalten. Beim Testen mit Unicode-Zeichen wurden zwei Verhaltensweisen bei der Momentaufnahmedifferenz festgestellt:

1. Der Befehl 'incremental' für die Momentaufnahmedifferenz wird mit dem Rückkehrcode 13001 beendet. Dieser Rückkehrcode tritt bei den Bereichen 'specials' und 'surrogate' von Unicode für Momentaufnahmedifferenzdatenträger auf, die mit UTF8-Flag erstellt wurden. Dieser Momentaufnahmedifferenzfehler tritt häufiger ohne UTF8-Flag auf. IBM Spectrum Protect wird mit der Fehlernachricht ANS5283E „Die Operation war nicht erfolgreich" beendet. Es werden keine Dateien gesichert.
2. Die Momentaufnahmedifferenz-API schlägt nicht fehl, aber gibt Zeichen zurück, die nicht Teil des realen Namens sind. IBM Spectrum Protect überprüft die Zeichenfolge, um zu bestimmen, ob sich Zeichen außerhalb des 7-Bit-ASCII-Bereichs befinden. Ist dies der Fall, überspringt IBM Spectrum Protect die Datei und protokolliert den Fehler in der Datei `dsmerror.log`.

Nachfolgend werden Situationen beschrieben, in denen Dateien und Verzeichnisse möglicherweise nicht gesichert werden und keine Fehler zurückgemeldet werden:

- Sie schließen eine Datei aus, indem Sie der Einschluss-/Ausschlussdatei eine Ausschlussregel hinzufügen. IBM Spectrum Protect führt mit dieser aktiven Ausschlussregel eine Sicherung der aktuellen Momentaufnahme aus. Sie haben die Datei nicht geändert, entfernen jedoch die Regel, mit der die Datei ausgeschlossen wurde. Ein Befehl zur Ausführung einer Teilsicherung unter Verwendung der Momentaufnahmedifferenz mit der Option `snapdiff` erkennt nicht diese

Einschluss-/Ausschlussänderung, da er Dateiänderungen nur zwischen zwei Momentaufnahmen erkennt. Die Dateien selbst müssen sich geändert haben, damit die Momentaufnahmedifferenz-API die Änderung erkennt und IBM Spectrum Protect die Datei sichert.

- Sie haben der Optionsdatei eine Einschlussanweisung hinzugefügt. Diese Einschlussanweisung wird nur dann wirksam, wenn von der Momentaufnahmedifferenz-API erkannt wird, dass die Datei geändert wurde. Die Dateien werden möglicherweise nicht gesichert, da IBM Spectrum Protect während der Sicherungsoperation nicht jede Datei auf dem Datenträger überprüft.
- Sie löschen eine Datei explizit aus dem IBM Spectrum Protect-Bestand, indem Sie den Befehl **DSMC DELETE BACKUP** ausgeben. Die Momentaufnahmedifferenz-API erkennt nicht, dass eine Datei manuell aus IBM Spectrum Protect gelöscht wurde. Daher bleibt die Datei im Speicher ungeschützt. Die Datei ist so lange ungeschützt, bis sie auf dem Datenträger geändert wird und die Änderung von der Momentaufnahmedifferenz-API erkannt wird. Nachdem die Änderung erkannt wurde, signalisiert die Momentaufnahmedifferenz-API IBM Spectrum Protect, die Datei erneut zu sichern.
- Maßnahmenänderungen, wie z. B. die Änderung der Maßnahme von 'mode=modified' in 'mode=absolute' werden nicht erkannt. Der gesamte Dateibereich wird aus dem Bestand gelöscht. Die nicht erkannten Maßnahmen haben zur Folge, dass IBM Spectrum Protect eine Momentaufnahme erstellt, die als Quelle (Basis) verwendet werden soll, und es wird eine vollständige Teilsicherung ausgeführt.

Durch die Ausführung einer vollständigen Teilsicherung ohne die Option `snapdiff` werden diese Einschränkungen beseitigt. IBM Spectrum Protect steuert nicht, wie sich ein geändertes Objekt darstellt. Die Änderung von Objekten wird jetzt von der Momentaufnahmedifferenz-API gesteuert. Daher wird durch die Ausführung einer vollständigen Teilsicherung ohne die Option `SNAPDIFF` sichergestellt, dass alle Dateiänderungen erkannt werden.

Für die Momentaufnahmedifferenzverarbeitung können Sie die folgenden Trace-Flags verwenden:

- `enter`
- `exit`
- `general`
- `snapshot`
- `hci`
- `hci_detail`
- `diskmap`
- `diskmap_detail`
- `hdw`
- `hdw_detail`
- `bacache`
- `snapdiffdb`

AIX Linux

Eine Benutzer-ID und ein Kennwort für den Root auf dem Dateiserver myFiler.ibm.com definieren.

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

```
Kennwort
für Benutzer-ID "root@myFiler.ibm.com" eingeben: ********
Kennwort zur Bestätigung erneut eingeben:********
ANS0302I Erfolgreich ausgeführt.
```

AIX Linux

Eine Benutzer-ID und ein Kennwort für den Root auf dem Dateiserver myFiler.ibm.com definieren.

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

Probleme mit Momentaufnahmeverzeichnis für NetApp- oder N-Series-Dateisystemdatenträger beheben

Wenn ein über Network File System (NFS) bereitgestellter Datenträger oder ein über Common Internet File System (CIFS) zugeordneter Datenträger gesichert wird, werden alle Momentaufnahmen innerhalb des Verzeichnisses `snapshot` ebenfalls gesichert. Diese Sicherung schließt nicht gewünschte Momentaufnahmen ein, die wertvollen Speicherplatz belegen können. Die über NFS bereitgestellten oder über CIFS zugeordneten Datenträger können entweder NetApp- oder N-Series-Datenträger sein.

Um zu verhindern, dass nicht gewünschte Momentaufnahmen gesichert werden, verwenden Sie die NDMP-Sicherungsmethode (NDMP = Network Data Management Protocol). Sie können Ihre Daten auch mit der Clientoption `SNAPSHOTROOT` sichern oder eine Teilsicherung mit dem Befehl **`INCREMENTAL`** und der Option `SNAPDIFF` ausführen. Schließen Sie alternativ das Verzeichnis `snapshot` von allen Sicherungen aus.

Wichtig: Linux Falls Sie eine NetApp-Gesamtsicherung mit der Option `SNAPDIFF` ausführen und anschließend den NetApp-Datenträger mit dem NFS4-Verfahren an den Server anhängen, findet eine weitere NFS-Gesamtsicherung statt. Um eine Gesamtsicherung zu verhindern, verwenden Sie das nicht dokumentierte Testflag **SNAPDIFFINCR**. Hierdurch wird eine Teilverarbeitung für Einträge erzwungen, die bereits verarbeitet worden sind. Beispiel: `-test=snapdiffincr`.

Anmeldeprobleme bei Verwendung des Encrypted File System auf Betriebssystemen AIX beheben

AIX

Während der Anmeldeverarbeitung wird der EFS-Schlüsselspeicher (EFS = Encrypted File System) automatisch geöffnet, wenn das Schlüsselspeicherkennwort dem Anmeldekennwort des Benutzers entspricht.

Wenn das Anmeldekennwort für AIX nicht mit dem EFS-Schlüsselspeicherkennwort übereinstimmt, müssen Sie den Schlüsselspeicher manuell öffnen, bevor Sie den Client starten. Öffnen Sie den Schlüsselspeicher, indem Sie den folgenden Befehl ausgeben:

```
efskeymgr -o <Befehl>
```

Starten Sie den Client mit einer der folgenden Methoden:

- Starten Sie den Befehlszeilenclient, indem Sie den Befehl `efskeymgr -o ./dsmc` ausgeben.

- Starten Sie den Java-GUI-Client, indem Sie den Befehl `efskeymgr -o ./dsmj` ausgeben.

Wenn Sie die Web-GUI (GUI - grafische Benutzerschnittstelle) des Clients verwenden, müssen Sie die Kennwörter synchronisieren. Geben Sie den folgenden Befehl aus, um das Benutzerkennwort mit dem EFS-Schlüsselspeicherkennwort zu synchronisieren:

```
efskeymgr -n
```

Imagesicherungsfehler beheben

AIX Linux

Imagesicherungsfehler können bei Linux-Images, Linux-Momentaufnahmeimages oder bei der momentaufnahmebasierten AIX JFS2-Sicherung/Archivierung und -Imagesicherung auftreten.

Linux-Imagesicherungsfehler beheben

Linux

Sie können Linux-Imagesicherungsfehler beheben, indem Sie, abhängig vom Typ des aufgetretenen Fehlers, bestimmte Schritte ausführen.

Informationen zu diesem Vorgang

Der folgende Fehler wurde während der Imagesicherung generiert:

```
paris:#dsmc b image /dev/system/lv01
Sicherungsimagefunktion aufgerufen.
ANS1228E Senden des Objekts '/dev/system/lv01' fehlgeschlagen
ANS1584E Fehler beim Laden der Systembibliothek 'libdevmapper.so',
die für Imageoperationen für LVM2-Datenträger erforderlich ist.
ANS1813E Die Verarbeitung der Imagesicherung von '/dev/system/lv01'
wurde mit Fehlern beendet.
Gesamtzahl geprüfter Objekte: 1
Gesamtzahl gesicherter Objekte: 0
Gesamtzahl aktualisierter Objekte: 0
Gesamtzahl erneut gebundener Objekte: 0
Gesamtzahl gelöschter Objekte: 0
Gesamtzahl verfallener Objekte: 0
Gesamtzahl fehlgeschlagener Objekte: 1
Gesamtzahl übertragener Byte: 0 B
Datenübertragungszeit: 0,00 s
Datenübertragungsgeschwindigkeit im Netz: 0,00 KB/s
Gesamtdatenübertragungsgeschwindigkeit: 0,00 KB/s
Objekte komprimiert um: 0 %
Abgelaufene Verarbeitungszeit: 00:00:29
paris# cat dsmerror.log
11/15/2006 13:07:53 ANS1228E Senden des Objekts
'/dev/system/lv01' fehlgeschlagen
11/15/2006 13:07:56 ANS1584E Fehler beim Laden der Systembibliothek
'libdevmapper.so', die für Imageoperationen für LVM2-Datenträger
erforderlich ist.
11/15/2006 13:07:56 ANS1813E Die Verarbeitung der Imagesicherung
von '/dev/system/lv01' wurde mit Fehlern beendet.
```

Stellen Sie bei diesem Fehler sicher, dass auf dem System die korrekte Version des Device-Mappers für Bibliotheken installiert ist. Führen Sie die folgenden Schritte aus, um die installierte Version zu bestimmen:

Vorgehensweise

1. Geben Sie den Befehl **# DMSETUP VERSION** aus. Die Ausgabe sieht in etwa wie folgt aus:

   ```
   Bibliotheksversion: 1.00.09-ioctl (2004-03-31)
   Treiberversion: 4.4.0
   ```

   oder

   Geben Sie den folgenden Befehl aus, um die Version zu bestimmen, die rpm verwendet:

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

   Die Ausgabe sieht in etwa wie folgt aus:

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

   Die Bibliothek muss Version 1.01 oder höher haben.
2. Überprüfen Sie nach dem Upgrade die Installation.

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

   Sie können auch durch Überprüfen des Verzeichnisses /lib feststellen, ob die korrekten Versionen installiert sind. Für ein System mit den korrekten Versionen würden die folgenden Informationen angezeigt:

   ```
   # 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
   ```

Sicherungsfehler bei Verwendung der Linux-Momentaufnahmeimagesicherung beheben

Linux

Um eine fehlgeschlagene Linux-Momentaufnahmeimagesicherung zu beheben, stellen Sie sicher, dass das System zum Erstellen einer Momentaufnahme konfiguriert ist.

Vorbereitende Schritte

Versuchen Sie, über eine Shellbefehlseingabeaufforderung eine Momentaufnahme zu erstellen, indem Sie den folgenden Befehl ausgeben:

```
/sbin/lvcreate -L 16384K -n <Momentaufnahmename z. B. tsmsnap>-s
<Datenträger Einheitenname z. B. /dev/system/lv01>
```

Wenn Sie den Fehler `Snapshot: Required device-mapper target(s) not detected in your kernel` empfangen, wurde das Kernelmodul **:dm_snapshot** nicht geladen. Dieser Befehl könnte auch aus anderen Gründen fehlschlagen, die ein ähnliches Verhalten von IBM Spectrum Protect zur Folge haben könnten.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt die Ausgabe, die generiert wird, wenn eine Imagesicherung mit Fehlernachricht ANS1258E, „Die Imagemomentaufnahmeoperation ist fehlgeschlagen", fehlschlägt.

```
dsmerror.log :
05/31/2006 15:14:36 ANS1259E Die Imagemomentaufnahmeoperation ist fehlgeschlagen.
Diagnosetext: tsmStartSnapshot.
05/31/2006 15:14:38 ANS1259E Die Imagemomentaufnahmeoperation ist fehlgeschlagen.
Diagnosetext: tsmTerminateSnapshot.
05/31/2006 15:14:38 ANS1228E Senden des Objekts '/fs1' fehlgeschlagen.
05/31/2006 15:14:38 ANS1258E Die Imagemomentaufnahmeoperation ist fehlgeschlagen.
```

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Module zu laden:

1. Stellen Sie sicher, dass das Modul nicht geladen ist. Siehe den folgenden Beispielbefehl:

   ```
   # lsmod |grep dm_
   dm_mod 112104 6
   ```

2. Laden Sie das Modul. Siehe den folgenden Beispielbefehl:

   ```
   # modprobe dm_snapshot
   ```

3. Stellen Sie sicher, dass der vorherige Schritt erfolgreich ausgeführt wurde. Siehe den folgenden Beispielbefehl:

   ```
   # lsmod |grep dm_
   dm_snapshot 44024 0
   dm_mod 112104 6 dm_snapshot
   #
   ```

4. Erstellen Sie über die Shelleingabeaufforderung eine Momentaufnahme. Siehe den folgenden Beispielbefehl:

   ```
   # /sbin/lvcreate -L 16384K -n tsmsnap -s /dev/system/lv01
   Logical volume „tsmsnap" created
   ```

5. Entfernen Sie die Momentaufnahme, die im vorherigen Schritt erstellt wurde. Siehe den folgenden Beispielbefehl:

   ```
   # lvremove /dev/system/tsmsnap
   Do you really want to remove active logical volume „tsmsnap"? [y/n]: y
   Logical volume "tsmsnap" successfully removed
   #
   ```

Ergebnisse

Wenn Sie alle Schritte ausgeführt haben, können Sie jetzt wahrscheinlich Momentaufnahmeimagesicherungen ausführen.

Einschränkung: Wenn der Befehl **`lvcreate`** mit dem Fehler „`Insufficient free extents (0) in volume group...`" fehlschlägt, ist in der Datenträgergruppe nicht genügend Speicherbereich für einen Momentaufnahmedatenträger vorhanden.

Fehler während der AIX-JFS2-momentaufnahmebasierten Sicherung/Archivierung und Imagesicherung beheben

AIX

Während der Beendigung von IBM Spectrum Protect löscht der Client die AIX JSF2-Momentaufnahme (JSF2 = Enhanced Journaled File System), die während des Sicherungsprozesses erstellt wird. Es gibt jedoch Situationen, in denen AIX die von IBM Spectrum Protect erstellte Anforderung zum Löschen der Momentaufnahme möglicherweise nicht ausführen kann.

Vorbereitende Schritte

Die folgenden Situationen veranschaulichen, wann eine Anforderung zum Löschen der Momentaufnahme fehlschlagen kann:

- Die Tastenkombination `Steuertaste-C` wird während eines IBM Spectrum Protect-Momentaufnahmesicherungsprozesses ausgegeben. Die Anforderung zum Abhängen der JFS2-Momentaufnahme kann mit einem Fehler „Einheit ausgelastet" fehlschlagen, weil der IBM Spectrum Protect-Prozess gerade dabei ist, auf die Momentaufnahme zuzugreifen.
- Zwei IBM Spectrum Protect-Momentaufnahmesicherungsanforderungen werden gleichzeitig für dasselbe Dateisystem gestartet. Beispielsweise wird die Sicherungsanforderung `dsmc backup image /fs1` von einer Konsole aus übergeben und gleichzeitig wird eine Sicherungsanforderung `dsmc backup image /fs1` von einer anderen Konsole aus ausgegeben. Wenn der Prozess von der ersten Konsole die erste Momentaufnahme für `/fs1` erstellt und der zweite Prozess von der zweiten Konsole die zweite Momentaufnahme für `/fs1` erstellt und dabei der zweite Prozess vor dem ersten Prozess beendet wird und versucht, die Momentaufnahme zu löschen, kann AIX die Löschanforderung nicht ausführen.
- Zwei IBM Spectrum Protect-Momentaufnahmesicherungsanforderungen werden gleichzeitig für zwei virtuelle Mountpunkte gestartet, die dasselbe Quellendateisystem haben. Beispielsweise wird `dsmc incr /fs1/level1/dir1` von einer Konsole und `dsmc incr /fs1/level2/level3/dir3` gleichzeitig von einer zweiten Konsole ausgegeben.

Informationen zu diesem Vorgang

AIX erwartet, dass Anforderungen zum Löschen von Momentaufnahmen in einer bestimmten Reihenfolge ausgegeben werden, wobei das Löschen der ältesten Momentaufnahme zuerst angefordert wird, gefolgt von der Anforderung zum Löschen der zweitältesten Momentaufnahme usw. Wenn IBM Spectrum Protect die Reihenfolge aufgrund gleichzeitig ablaufender Prozesse, die Momentaufnahmen für dasselbe Dateisystem erstellen, nicht akzeptieren kann, kann AIX die Löschanforderungen nicht ausführen. In den vorherigen Beispielen protokolliert IBM Spectrum Protect eine Warnung, die den Benutzer dazu auffordert, die Momentaufnahmen manuell zu löschen.

Vorgehensweise

Geben Sie zum manuellen Löschen einer Momentaufnahme die folgenden Befehle in dieser Reihenfolge aus:

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

   Wenn der Prozess zum Löschen von Momentaufnahmen mit der Fehlernachricht „Einheit ausgelastet" oder einer anderen Fehlernachricht fehlschlägt, geben Sie den Befehl `- unmount -f <srcfs>` aus, um das Quellendateisystem abzuhängen. Versuchen Sie anschließend erneut, die Momentaufnahme zu löschen.
6. `ls -l /dev/tsm*`

   Wenn logische Datenträger `/DEV/TSM*` nicht gelöscht werden, geben Sie den Befehl `- rmlv -f tsm*` aus.

7. Wenn ein nicht angehängtes Quellendateisystem vorhanden ist, geben Sie den Befehl - `mount <srcfs>` aus, um es anzuhängen.

Ergebnisse

Wenn während eines vorherigen IBM Spectrum Protect-Prozesses nicht alle Momentaufnahmen gelöscht wurden, versucht IBM Spectrum Protect, die Momentaufnahmen während des nächsten Aufrufs zu löschen, da AIX - weil ältere Momentaufnahmen nicht gelöscht wurden - Löschanforderungen für neuere Momentaufnahmen für ein Dateisystem nicht ausführen kann. Nachfolgend sind Fälle aufgeführt, in denen IBM Spectrum Protect nicht versucht, ältere Momentaufnahmen zu löschen:

- Wenn die Momentaufnahme nicht von IBM Spectrum Protect erstellt wurde, ordnet IBM Spectrum Protect seinen Momentaufnahmen das Präfix „tsm" zu, um sie von anderen Momentaufnahmen, die für dasselbe Dateisystem erstellt werden, zu unterscheiden. Wenn die Momentaufnahme nicht von IBM Spectrum Protect erstellt wurde, wird eine Fehlernachricht generiert, die den Benutzer dazu auffordert, die ältere Momentaufnahme zu löschen und die Operation zu wiederholen.
- Wenn die Momentaufnahme von IBM Spectrum Protect erstellt wird, aber noch angehängt ist, wird die Momentaufnahme von einem anderen IBM Spectrum Protect-Prozess verwendet.
- Wenn die Momentaufnahme von IBM Spectrum Protect erstellt wird, nicht angehängt ist, aber neu erstellt wird, wurde die Momentaufnahme möglicherweise von einem anderen IBM Spectrum Protect-Prozess erstellt.

In allen derartigen Fällen müssen Sie unter Umständen einen manuellen Löschvorgang ausführen. Wenn ältere nicht verwendete Momentaufnahmen vorhanden sind, können nachfolgende IBM Spectrum Protect-Sicherungen keine Momentaufnahmen löschen.

Wichtig: Es sind zwei AIX-Fehlerkorrekturen vorhanden, die für JFS2-Momentaufnahmen in AIX 6.1 oder höher gelten. Wenn die Korrekturen nicht angewendet werden, kann ein AIX-Systemabschluss auftreten oder IBM Spectrum Protect wird möglicherweise während der Prozesse zum Löschen und Abfragen von Momentaufnahmen gestoppt. Außerdem kann dies während der Imagesicherung verwendeter Blöcke zum Datenverlust führen. IBM Spectrum Protect führt daher die folgenden Tasks nicht aus:

- Überwachung von Momentaufnahmen
- Löschung von Momentaufnahmen

Um diese Funktionen nutzen zu können, müssen Sie sicherstellen, dass Ihre Betriebssystemversion AIX 6.1 oder höher ist.

Unterstützung für die IBM Spectrum Protect-API

Es stehen Ressourcen zur Verfügung, die die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) beschreiben und mit denen die API diagnostiziert werden kann.

Die API-Instrumentierung ist nur aktiviert, wenn die API `testflag INSTRUMENT:` in der Konfigurationsdatei definiert ist und die Aufrufe **`dsmSetUp`** und **`dsmCleanUp`** in der Anwendung verwendet werden.

Weitere Informationen finden Sie in *Verwendung der Anwendungsprogrammierschnittstelle* oder IBM Support Assistant.

API-Informationen zusammenstellen, bevor der IBM Support benachrichtigt wird

Sie können bei der Bestimmung eines API-Fehlers in hohem Maße helfen, indem Sie Informationen zu Ihrer Umgebung erfassen.

Stellen Sie möglichst viele der folgenden Informationen zusammen, bevor Sie den IBM Support benachrichtigen:

- Unter welchem Betriebssystem ist der Fehler aufgetreten?
- Welche Version des Betriebssystems, einschließlich aller angewendeten Service-Packs und Hotfixes, wird verwendet?
- Welche Version der IBM Spectrum Protect-API wird verwendet?
- Welche Version des IBM Spectrum Protect-Servers wird verwendet?
- Welche IBM Spectrum Protect-Serverplattform und Betriebssystemversion wird verwendet?
- Welche Version des IBM Spectrum Protect-Speicheragenten (in LAN-unabhängiger Umgebung) wird verwendet?
- Welche Plattform und Betriebssystemversion wird für den IBM Spectrum Protect-Speicheragenten (in LAN-unabhängiger Umgebung) verwendet?
- Welche Anwendungen werden auf dem System ausgeführt?
- Welche Schritte sind erforderlich, um das Problem zu reproduzieren? Kann der Fehler nicht reproduziert werden, welche Schritte haben den Fehler verursacht?

API-Dateien zusammenstellen, bevor der IBM Support benachrichtigt wird

Protokolldateien und andere wichtige Daten werden von der IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) erstellt.

Stellen Sie möglichst viele der folgenden Dateien zusammen, bevor Sie den IBM Support benachrichtigen:

- IBM Spectrum Protect-API-Fehlerprotokolldatei. Die API-Standardfehlerprotokolldatei ist `dsierror.log`.
- Alle gegebenenfalls für die API erstellten Tracedateien. Die Trace-Flags lauten normalerweise `api`, `api_detail` oder `verbdetail`.
- Ausgabe von allen fehlgeschlagenen Befehlen oder Operationen. Dies kann entweder die Konsolausgabe, die in eine Datei umgeleitet wurde, oder ein tatsächliches Anzeigenimage des Fehlers sein.
- Die Ausgabe des Serverbefehls **`QUERY SYSTEM`**.
- Die Serveraktivitätenprotokolldatei. Der IBM Spectrum Protect-Administrator kann diese Protokolldatei für Sie anzeigen, wenn Sie keine IBM Spectrum Protect-Administrator-ID und kein Kennwort haben.
- Ist der API-Client für die LAN-unabhängige Datenversetzung konfiguriert, suchen Sie die Optionsdatei für den IBM Spectrum Protect-Speicheragenten. Die Optionsdatei heißt standardmäßig `dsmsta.opt`.
- Ein kurzes Programm oder Abschnitte des Anwendungsquellcodes, mit dem die IBM Spectrum Protect-API-Funktionsaufrufe aufgerufen werden und die als Verursacher des Fehlers vermutet werden.
- IBM Spectrum Protect-API-Optionsdatei.

Die beiden folgenden Optionsdateien werden unter den Betriebssystemen Linux und UNIX verwendet:

dsm.opt
Die Clientoptionsdatei

dsm.sys
Die Systemoptionsdatei

Suchen Sie für Windows die Standardoptionsdatei `dsm.opt` oder die Datei, auf die durch die Umgebungsvariable **DSMI_CONFIG** verwiesen wird. Für Linux und UNIX ist die Standardoptionsdatei `dsm.sys`. Sie befindet sich in dem Verzeichnis, auf das durch die Umgebungsvariable **DSMI_DIR** verwiesen wird.

Auf anderen Betriebssystemen enthält die Clientoptionsdatei `dsm.opt` alle Optionen. Die folgenden Definitionen sind Umgebungsvariablen, die die Position der Optionsdateien und andere API-Komponenten beschreiben:

DSMI_CONFIG
Der vollständig qualifizierte Name für die Clientoptionsdatei.

DSMI_DIR
Die Variable *DSMI_DIR* verweist auf das API-Installationsverzeichnis und wird auch verwendet, um die Datei `dsm.sys` unter Linux und UNIX zu lokalisieren. Wo immer *DSMI_DIR* definiert ist, stellen Sie sicher, dass eine Datei `dsm.sys` in demselben Verzeichnis vorhanden ist.

DSMI_LOG
Die Variable *DSMI_LOG* verweist auf den Pfad für die Datei `dsierror.log`. Falls die Clientoption `errorlogname` festgelegt ist, überschreibt die mit dieser Option angegebene Position das Verzeichnis, das durch *DSMI_LOG* angegeben ist.

Tipp: Wenn die Variable *DSMI_LOG* auf ein Verzeichnis verweist, für das der Benutzer keine Schreibberechtigung hat, schlagen **dsmSetup** und **dsmInitEx** mit dem Rückkehrcode `DSM_RC_ACCESS_DENIED (106)` fehl.

Ist die Option `errorlogname` in der Optionsdatei `dsm.sys/dsm.opt` definiert, wird ihr Wert anstelle des Standardwerts `dsierror.log` als Fehlerprotokollname verwendet.

Verwendung der korrekten Optionsdatei durch die API überprüfen

AIX Linux Mac OS X

Wenn Sie Dateien der Anwendungsprogrammierschnittstelle (API) zusammenstellen, müssen Sie überprüfen, ob die API die korrekte Optionsdatei oder Serverzeilengruppe in `dsm.sys` verwendet.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob die API die korrekte Optionsdatei oder Serverzeilengruppe verwendet:

1. Fügen Sie eine fehlerhafte Option oder einen fehlerhaften Wert in die Clientoptionsdatei bzw. die Serverzeilengruppe in `dsm.sys` ein. Sind Sie beispielsweise nicht sicher, ob die API den Server `srvr1.cmpron` verwendet, fügen Sie die Anweisung 'ERRONEOUS_OPTION 12345' in die Serverzeilengruppe `srvr1.cmpron` der Datei `dsm.sys` ein. Siehe das folgende Beispiel:

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

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

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

2. Überprüfen Sie, ob die API den Fehler erkennt. Sie können das API-Musterprogramm `dapismp` für diesen Zweck verwenden.

```
# dapismp
...
Enter selection ==>0
Node name:node1
Owner name:
Password:
API Config file:
Session options:
User Name:
User pswd:
Are the above responses correct (y/n/q)?
Doing signon for node node1, owner, with password
*** Init failed: ANS0220E (RC400) An invalid option was found during option parsing.
```

   Wenn kein Fehler zurückgemeldet wird, wurde die falsche Optionsdatei aktualisiert.

3. Überprüfen Sie die Werte der in „API-Dateien zusammenstellen, bevor der IBM Support benachrichtigt wird" auf Seite 37 aufgeführten Umgebungsvariablen oder wiederholen Sie die Schritte 1 und 2 mit einer anderen Optionsdatei oder Serverzeilengruppe.
4. Entfernen Sie die in Schritt 1 eingefügte Option.

Speicheragent statt Server als Sendeziel für Daten feststellen

Sie müssen wissen, ob Ihre Daten statt an einen Server an den IBM Spectrum Protect-Speicheragenten gesendet werden. Wenn die Daten an den Speicheragenten gesendet werden, können Sie die Daten nicht wiederherstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob Daten statt an den Server an den IBM Spectrum Protect-Speicheragenten gesendet werden:

1. Fügen Sie der Clientoptionsdatei die folgenden Traceoptionen hinzu, bevor Sie Objekte sichern oder archivieren:
   - `TRACEFILE <`*`Tracedateiname`*`>`
   - `TRACEFLAGS api api_detail verbdetail`
2. Überprüfen Sie die Tracedatei nach der Operation und suchen Sie eine Anweisung, die ähnlich wie die folgende aussieht:

   ```
   dsmSendObj ENTRY:... objNameP: '<Dateiname>'
   ```

   Auf diese Anweisung folgt die folgende Traceanweisung:

```
tsmEndSendObjEx: Total bytes sent * *, encryptType is *** encryptAlg is
*** compress is *, totalCompress is * * totalLFBytesSent * *
```

Die Traceanweisung gibt an, ob das Objekt **totalLFBytesSent** an den IBM Spectrum Protect-Speicheragenten gesendet wurde. Ist **totalLFBytesSent** 0 0, wurden die Daten direkt an den IBM Spectrum Protect-Server gesendet.

Stattdessen kann auch Ihre Anwendung über den Funktionsaufruf **dsmEndSendObjEx** und die Datenstruktur **dsmEndSendObjExOut_t** selbst bestimmen, ob die Daten über einen LAN-unabhängigen Pfad gesendet wurden.

```
/*-------------------------------------------------------------------------+
| Typdefinition für dsmEndSendObjExOut_t
+-------------------------------------------------------------------------*/
typedef       struct       dsmEndSendObjExOut_t
{
dsUint16_t     stVersion; /* Strukturversion */
dsStruct64_t   totalBytesSent; /* Gesamtsumme aus Anwendung gelesener Byte */
dsmBool_t      objCompressed;  /* mit Objektkomprimierung */
dsStruct64_t   totalCompressSize;  /* Gesamtgröße nach Komprimierung */
dsStruct64_t   totalLFBytesSent;  /* Gesamtanzahl LAN-unabhängig gesendeter Byte */
dsUint8_t      encryptionType; /* verwendeter Verschlüsselungstyp */
 }dsmEndSendObjExOut_t;
  totalLFBytesSent - Die Gesamtanzahl empfangener LAN-unabhängiger Byte.
```

Beispiel:

```
...
    rc = dsmEndSendObjEx(&endSendObjExIn, &endSendObjExOut);
    if (rc)
 {
          printf("*** dsmEndSendObjEx fehlgeschlagen: ");
     rcApiOut(dsmHandle, rc);
 }
 else
 {
          dI64toCh(&endSendObjExOut.totalLFBytesSent,t,10);
          format_number(t,t2);
          printf("LAN-unabhängig gesendete Byte: %s\n", t2);
```

Nächste Schritte

Weitere Details finden Sie unter *API-Funktionsaufrufe* im Handbuch *Verwendung der Anwendungsprogrammierschnittstelle*.

Anwendungen ausführen, die die API als Benutzer-ID ohne Rootberechtigung verwenden

AIX Linux Mac OS X

Sie müssen bestimmte Schritte ausführen, wenn Sie mit einer Benutzer-ID ohne Rootberechtigung angemeldet sind und versuchen, eine Anwendung auszuführen, die die Anwendungsprogrammierschnittstelle (API) verwendet.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einer Benutzer-ID ohne Rootberechtigung den Zugriff auf die API zu ermöglichen:

1. Definieren Sie die Umgebungsvariable **DSMI_CONFIG**. Stellen Sie sicher, dass die Benutzer-ID ohne Rootberechtigung für die durch DSMI_CONFIG angegebene Clientoptionsdatei über Leseberechtigung verfügt. Andernfalls schlägt dsmInit/dsmInitEx mit Rückkehrcode DSM_RC_NO_OPT_FILE (406) fehl. Die fol-

gende Optionsdatei kann beispielsweise von einer Benutzer-ID ohne Rootberechtigung nicht gelesen werden; daher müssen die Dateiberechtigungen aktualisiert werden:

```
$ ls -l $DSMI_CONFIG
-rwx------   1 root    sys    86 Oct 7 13:07 /testfsapi/callmt_nr/dsm.opt
$ su root
Password:
# 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. Setzen Sie die Umgebungsvariable **DSMI_DIR** auf das API-Installationsverzeichnis. Stellen Sie sicher, dass die Benutzer-ID ohne Rootberechtigung für die durch $DSMI_DIR/dsm.sys angegebene Systemoptionsdatei über Leseberechtigung verfügt.

   ```
   $ 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. Definieren Sie die Umgebungsvariable **DSMI_LOG**. Stellen Sie sicher, dass die Benutzer-ID ohne Rootberechtigung für dieses Verzeichnis über Schreibberechtigung verfügt. Beispielsweise ist eine Benutzer-ID ohne Rootberechtigung Eigner des folgenden in DSMI_LOG angegebenen Verzeichnisses:

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

   Wenn **PASSWORDACCESS GENERATE** in der Systemoptionsdatei dsm.sys definiert ist, führen Sie die Schritte 4 und 5 aus; fahren Sie andernfalls mit Schritt 6 fort.

4. Optional: Überprüfen Sie das Eigentumsrecht und die Berechtigungen von Trusted Communication Agent (TCA) nur dann, wenn die Option PASSWORDDIR nicht verwendet wird oder auf ein Verzeichnis verweist, für das der Benutzer keinen Schreib-/Lesezugriff besitzt. Diese Datei befindet sich in dem Verzeichnis, das durch die Umgebungsvariable **DSMI_DIR** angegeben wird. Beispielsweise hat der folgende TCA das korrekte Eigentumsrecht und die korrekten Berechtigungen:

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

   Falsche Berechtigungen oder ein falsches Eigentumsrecht haben zur Folge, dass DSM_RC_AUTH_FAILURE (137) von dsmInit zurückgegeben gibt. Außerdem ist es zwingend erforderlich, dass die API-Bibliothek und dsmtca dieselbe Version haben. Unterschiedliche Versionen haben Fehler zur Folge.

   ```
   Error : calling program and dsmtca are not compatible
   calling program build date : Mon Oct 18 21:15:59 2004 Mon Oct 18 21:15:59 2004
   TCA build date : Wed Oct 13 16:48:03 2004 Wed Oct 13 16:48:03 2004
   *** Init failed: ANS0282E (RC168) Password file is not available.
   ```

5. Der Rootbenutzer oder der berechtigte Benutzer muss die Kennwortdatei TSM.PWD entweder mit dem Client für Sichern/Archivieren oder der API-Musteranwendung **dapismp** generieren. Ein berechtigter Benutzer ist jede Benutzer-ID ohne Rootberechtigung, die Schreib-/Lesezugriff auf das gespeicherte Kennwort (Datei TSM.PWD) hat. Die Position für die Kennwortdatei wird durch die Option PASSWORDDIR in der Systemoptionsdatei dsm.sys festgelegt. In dem folgenden Beispiel wird mit der API-Musteranwendung die Kennwortdatei TSM.PWD für einen Knoten mit dem Kennwort *oddesy* generiert:

```
# dapismp
********************************************************************************
* Welcome to the sample application for the IBM Spectrum Protect API. *
* API Library Version = 5.4.0.0 *
********************************************************************************
Choose one of the following actions to test:
0. Signon
1. Backup
2. Restore
3. Archive
4. Retrieve
5. Queries
6. Change Password
7. Utilities : Deletes, Updates, Logevent, SetAccess, RetentionEvent
8. Set preferences, envSetUp
9. Exit to system
10. Restore/Retrieve Without Offset Prompt
11. Extended Signon
Enter selection ==>0
Node name:
Owner name:
Password:oddesy
API Config file:
Session options:
User Name:
User pswd:
Are the above responses correct (y/n/q)?
Doing signon for node, owner, with password oddesy
Handle on return = 1
Choose one of the following actions to test:
0. Signon
1. Backup
2. Restore
3. Archive
4. Retrieve
5. Queries
6. Change Password
7. Utilities : Deletes, Updates, Logevent, SetAccess, RetentionEvent
8. Set preferences, envSetUp
9. Exit to system
10. Restore/Retrieve Without Offset Prompt
11. Extended Signon
Enter selection ==>9
# ls -l TSM.PWD
-rw------- 1 root sys 121 Oct 19 18:28 TSM.PWD
Function call dsmInit returns DSM_RC_NO_PASS_FILE (168), if the password
file is not present in the directory specified by the PASSWORDDIR option.
```

6. Wenn die Tracefunktion aktiviert ist, überprüfen Sie, ob die Benutzer-ID ohne Rootberechtigung für die mit der Option TRACEFILE angegebene Datei über Schreibberechtigung verfügt.

Fehlerbestimmung für journalbasierte Sicherungen

Windows

Die journalbasierte Sicherung (Journal Based Backup, JBB) ist für die Sicherung von Dateisystemen mit geringer oder mäßiger Änderungsaktivität zwischen Sicherungszyklen geeignet.

Bestimmen, ob eine Sicherung journalbasiert sein wird

Windows

Bevor Sie eine Sicherung implementieren, müssen Sie bestimmen, ob die Sicherung journalbasiert sein wird.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass die Sicherung journalbasiert ist:

Vorgehensweise

1. Konfigurieren Sie den Journaldämon für die Aufzeichnung des Dateisystems, das gesichert wird. Der Journaldämon zeichnet ein Dateisystem auf, nachdem Sie das Dateisystem in der Konfigurationsdatei `tsmjbbd.ini` aufgelistet haben. Siehe die folgenden Konfigurationsdaten:

   ```
   [JournaledFileSystemSettings]
   ;
   ; Liste der aufgezeichneten Dateisysteme
   JournaledFileSystems=c:
   ```

2. Führen Sie eine vollständige Teilsicherung für das entsprechende Dateisystem aus, während das Dateisystem aktiv aufgezeichnet wird. Diese vollständige Teilsicherung muss das Datum für die „letzte abgeschlossene Sicherung" im IBM Spectrum Protect-Serverdateibereich setzen, damit das Journal auf 'Gültig' gesetzt wird. Sie können das Datum für die „letzte abgeschlossene Sicherung" anzeigen, indem Sie den Serverbefehl **QUERY FILESPACE** ausgeben. Nachdem das Journal auf den Status 'Gültig' gesetzt wurde, sind nachfolgende Sicherungen, die von demselben Knoten auf denselben Server ausgeführt werden, journalbasiert. Wenn für eine Sicherung ein anderer Knoten oder ein anderer Server verwendet wird, ist die Sicherung zwar nicht journalbasiert, das Journal bleibt jedoch für den ursprünglichen Knoten gültig und Sicherungen mit dem ursprünglichen Knoten und dem ursprünglichen Server sind weiterhin journalbasiert.

   Die folgende Nachricht ist ein Beispiel für die Ausgabe, die in das Windows-Anwendungsereignisprotokoll geschrieben wird, wenn ein Journal anfänglich auf 'Gültig' gesetzt wird:

   ```
   Journal für Dateisystem 'H:' auf 'Gültig' gesetzt; Journal wird für
   Sicherung von Knoten GSHLAGER3 auf Server GSHLAGER2_SERVER1 verwendet.
   ```

3. Stellen Sie sicher, dass der IBM Spectrum Protect-Knoten und -Server, die von der Sicherung verwendet werden, mit dem Knoten und Server übereinstimmen, für die das Journal gültig ist.

4. Verwenden Sie das Dienstprogramm zum Anzeigen der Journaldatenbank (Journal Database Viewing), um den aktuellen Status eines Journals zu bestimmen. Wenn ein gültiges Journal erneut gestartet wird, sind Sicherungen so lange nicht journalbasiert, bis das Journal erneut validiert wird.

   Die folgende Nachricht wird in das Windows-Anwendungsereignisprotokoll geschrieben, wenn ein Journal erneut gestartet wird:

   ```
   Journaldatenbank 'c:\tsmjournal\tsmH__.jdb' für Dateisystem 'H:'
   wurde gelöscht und auf Status 'Ungültig' zurückgesetzt.
   ```

Gültiges Journal erneut starten

AIX Linux Windows

Sie können die Leistung erhöhen, indem ein gültiges Journal erneut gestartet wird.

Die Gründe für den Neustart eines gültigen Journals sind:

- Fehlerbedingungen im Journaldämon
  - Pufferüberlauffehler aufgrund von übermäßigen Änderungsaktivitäten im Journaldateisystem, das auf Änderungen überwacht wird
  - Journaldatenbankzugriffsfehler (Fehler wegen voller Platte, usw.)
- Anforderung durch einen Sicherungsclient
- Clients geben eine Anforderung zum Neustart eines Journals aus, wenn festgestellt wird, dass für ein Journaldateisystem aus einem der folgenden Gründe die Integrität fehlt:
  - Der Serverdateibereich ist nicht mehr vorhanden
  - Der Serverdateibereich wurde nach der letzten Sicherung gelöscht
  - Die Maßnahmengruppe des Knotens wurde nach der letzten Sicherung aktualisiert
  - Die Datumsangaben für 'Abschluss der letzten Sicherung' oder 'Start der letzten Sicherung' sind nicht gültig (nicht definiert)

Journaldämon im Vordergrund ausführen

Windows

Sie können die Diagnose- und Testfunktionalität verbessern, indem Sie den Journaldämon im Vordergrund und nicht als Windows-Dienst ausführen.

Starten Sie den Journaldämon wie folgt in einer Windows-Eingabeaufforderung:

```
tsmjbbd.exe i
```

Dienstprogramm zum Anzeigen der Journaldatenbank (Journal Database Viewing)

Windows

Das Dienstprogramm zum Anzeigen der Journaldatenbank (Journal Database Viewing Utility) stellt wertvolle Informationen für die Fehlerbestimmung bei journalbasierten Sicherungen bereit.

Das Dienstprogramm zum Anzeigen der Journaldatenbank stellt die folgenden Informationen zur Verfügung:

- Den aktuellen Status des Journals
- Das vom Journal überwachte Dateisystem
- Die Zeitmarke der Journalaktivierung
- Die Zeitmarke der Journalprüfung
- Die maximale unterstützte Journalgröße
- Den Knoten und Server, für die das Journal gültig ist
- Die aktuelle Anzahl Einträge im Journal

Anmerkung: Bei Clients für Sichern/Archivieren, die älter als Version 6.3.1 sind, können Sie den Inhalt von geöffneten Journalen nicht mit dem Dienstprogramm

zum Anzeigen einsehen. Ein geöffnetes Journal ist ein Journal, das von einem anderen Prozess (z. B. dem Journaldämon) geöffnet wird. Sie können jedoch den Inhalt des Steuerungsdatensatzes eines geöffneten Journals anzeigen. Das Dienstprogramm zum Anzeigen ist mit Clients für Sichern/Archivieren der Version 6.3.1 und neueren Clients für Sichern/Archivieren verfügbar. Weitere Informationen zum Dienstprogramm zum Anzeigen finden Sie in der folgenden Technote: Run the dbviewb.exe utility in batch mode.

Dieses Dienstprogramm ermöglicht auch das Durchsuchen, Einfügen oder Löschen bestimmter Einträge in einer Journaldatenbank.

Dieses Dienstprogramm hat folgende Syntax:

```
dbviewb <vollständig qualifizierter Basisdateiname der Journaldatenbank>
dbviewb <vollständig qualifizierter Basisdateiname der Journaldatenbank> <i>
```

```
D:\tsm540c\debug\bin\winnt_unicode>dbviewb c:\tsmjournal\tsmh__.jdb
IBM Spectrum Protect
Journal Database Viewing Utility
Version 5, Release 4, Level 0.0
Last Update: Nov 28 2006
Querying Journal DB ...
Journal Database Information:
Database File c:\tsmjournal\tsmh__.jdb
Database File Disk Size 81 KB (83754 Bytes)
Journal File System H:
Journal Activation Date Tue Nov 28 11:49:05 2006
Journal Validation Date Wed Nov 29 16:41:11 2006
Maximum Journal Size 8191 PB (9223372036854775807 Bytes)
Journal Type Change Journal
Journal State Valid
Valid for Server GSHLAGER2_SERVER1
Valid for Node GSHLAGER3
Number of DB Entries 22
D:\tsm540c\debug\bin\winnt_unicode>
```

```
D:\tsm540c\debug\bin\winnt_unicode>dbviewb c:\tsmjournal\tsmh__.jdb i
IBM Spectrum Protect
Journal Database Viewing Utility
Version 5, Release 4, Level 0.0
Last Update: Nov 28 2006
Querying Journal DB ...
Journal Database Information:
Database File c:\tsmjournal\tsmh__.jdb
Database File Disk Size 81 KB (83754 Bytes)
Journal File Syst em H:
Journal Activation Date Tue Nov 28 11:49:05 2006
Journal Validation Date Wed Nov 29 16:41:11 2006
Maximum Journal Size 8191 PB (9223372036854775807 Bytes)
Journal Type Change Journal
Journal State Valid
Valid for Server GSHLAGER2_SERVER1
Valid for Node GSHLAGER3
Number of DB Entries 22
Enter request on a single line, in the following format:
Req-Type [Entry-key]
Req-type might be one of the following:
Del Delete a row from the database. The fully-qualified case sensitive
file name is required.
Find Find the entry whose key is the argument.
List Print all the entries to stdout. No arguments are required.
Quit
Please enter your request: find H:\dbview.example\Dir3Depth1\F2.txt
Located Journal Database Record:
----------------------------------------
Object Name : H:\dbview.example\Dir3Depth1\F2.txt
Action : Modify
```

```
Object Type : File
Inserted : Fri Dec 01 10:15:28 2006
Object Time : Fri Dec 01 14:15:28 2006
Hit Count : -2110169276
----------------------------------------
Please enter your request: quit
```

Windows Volume Shadow Copy Service verwenden

Windows

Der IBM Spectrum Protect Windows-Client verwendet Volume Shadow Copy Service (VSS) zur Ausführung von Systemstatus- und Systemservicesicherungen. VSS kann auch als Momentaufnahmeprovider für OFS (Open File Support = Unterstützung offener Dateien) und Online-Imageoperationen verwendet werden.

Temporäre VSS-Fehler definieren

Windows

Der Client betrachtet verschiedene VSS-Fehler als temporäre Fehler. Temporäre Fehler sind Netzfehler oder Laufwerke, die vorübergehend nicht korrekt arbeiten und für die unter Umständen eine Wiederherstellung erforderlich ist.

Wenn einer dieser Fehler auftritt, versucht der Client standardmäßig, drei Mal in Intervallen von 30 Sekunden, den VSS-Sicherungsprozess zu wiederholen. Die Anzahl Neuversuche und das Intervall zwischen Neuversuchen kann mithilfe von zwei Testflags (**TESTFLAG SETVSSMAXRETRY** und **TESTFLAG SETVSSDELAY**) konfiguriert werden. Der Client betrachtet die folgenden VSS-Fehler als temporäre Fehler:

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

Windows-VSS-Testflags definieren

Windows

Der Client verwendet zwei unterschiedliche Testflags, um die Anzahl von VSS-Neuversuchen und das Intervall zwischen Neuversuchen zu konfigurieren.

Mithilfe der folgenden Testflags werden die Anzahl Neuversuche und das Intervall zwischen Neuversuchen für IBM Spectrum Protect definiert:

SETVSSMAXRETRY
Gibt an, wie oft ein Neuversuch für den VSS-Sicherungsprozess ausgeführt wird, wenn ein temporärer Fehler auftritt. Der Standardwert sind drei Neuversuche.

SETVSSDELAY
Gibt die Anzahl Sekunden an, die zwischen Neuversuchen des VSS-Sicherungsprozesses gewartet werden soll, wenn ein temporärer Fehler auftritt. Der Standardwert sind 60 Sekunden.

Beispiel für die Optionsdatei:

```
retry 10 times at 300 second intervals
TESTFLAG SETVSSMAXRETRY:10
TESTFLAG SETVSSDELAY:300
```

Volume Shadow Copy Service optimieren

Windows

Es sind verschiedene Fixes zur Optimierung des Microsoft Volume Shadow Copy Service (VSS) verfügbar, sollten Sie Probleme bei der Optimierung von VSS haben.

Größe von VSS-DiffArea steuern

Nachdem Sie diese Fixes angewendet haben, tritt eines der folgenden Ereignisse auf:

- „The shadow copy of volume C: took too long to install"
- „The shadow copy of volume C: was stopped because the diff area file could not grow in time."

Reduzieren Sie die E/A-Last auf diesem System, um diese Probleme zu vermeiden. Wenn die Ereignisse weiterhin auftreten, steuern Sie die Größe des von VSS verwendeten DiffArea mithilfe des folgenden Registrierungsschlüssels:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VolSnap\`
`MinDiffAreaFileSize : REG_DWORD: <Größe in MB>` (die Standardgröße ist 300, sie kann jedoch auf 3000 erhöht werden).

Maximale Größe des Ereignisprotokolls

Wenn die Ereignisprotokolle ausreichend groß sind, kann die Kopieroperation laut Aussage von Microsoft länger dauern, als für das Zeitlimit auf Systemen mit hoher E/A-Last oder hoher Speicherbelegung definiert ist. Der beste Wert für die Protokollgröße liegt bei weniger als 64 MB.

VSS-Diagnoseinformationen für die Unterstützung durch Microsoft zusammenstellen

Windows

Die IBM Diagnoseinformationen für VSS-Fehler (VSS = Volume Shadow Copy Service) enthalten möglicherweise nicht die erforderlichen Angaben. Diagnoseinformationen für VSS-Fehler finden Sie auf der Microsoft-Unterstützungssite.

Wenn der VSS-Fehler außerhalb von IBM Spectrum Protect liegt, stellen Sie für den Microsoft Support die folgenden Informationen zusammen:

- Windows-Anwendungsereignisprotokoll
- Windows-Systemereignisprotokoll
- VSS-Trace

Untersuchen Sie die Anwendungs- und Systemereignisprotokolldateien und legen Sie dabei den Schwerpunkt auf die Fehlerereignisse, die von den VolSnap- und VSS-Quellen zu dem Zeitpunkt erstellt wurden, zu dem der Fehler aufgetreten ist. Sie können die betreffenden Ereignisse aus dem Protokoll extrahieren, um das Problem einzugrenzen und so eine produktivere Interaktion mit dem Microsoft Support sicherzustellen.

Fehler mithilfe eines VSS-Trace beheben

Windows

Sie können Fehler des Volume Shadow Copy Service (VSS) beheben, indem Sie einen VSS-Trace ausführen.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um einen VSS-Trace auszuführen:

Vorgehensweise

1. Erstellen Sie eine Datei `tracing.reg` und ändern Sie den Eintrag TraceFile so, dass er auf einen Datenträger verweist, für den keine Spiegelkopie erstellt werden muss. Erstellen Sie die Datei mithilfe des Inhalts am Ende dieser Datei. Beachten Sie, dass Sie einen doppelten umgekehrten Schrägstrich als Begrenzer verwenden müssen; in dem Pfad, den Sie angeben möchten, müssen Sie „\\" als Begrenzer für jeden umgekehrten Schrägstrich in dem Pfad eingeben.
2. Klicken Sie in Windows Explorer doppelt auf die Datei `tracing.reg`, um diese zu installieren.
3. Reproduzieren Sie den Fehler.
4. Inaktivieren Sie die Tracefunktion, indem Sie den Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VSS\Debug\Tracing` löschen.

Ergebnisse

Der folgende Inhalt wird in der Registry-Datei `tracefile.reg` angezeigt:

```
Windows Registry Editor Version 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
```

VSS-API-Aufrufe mit dem Beispielprogramm vsreq.exe ausführen

Windows

Das Volume Shadow Copy Service (VSS) Software-Development-Kit (SDK) enthält das Beispielprogramm **vsreq** (VSS Requestor). Das Programm VSS Requestor führt eine Folge von VSS-API-Aufrufen auf dieselbe Art und Weise aus, wie die Aufrufe vom Client für Sichern/Archivieren ausgeführt werden.

Sie können `vsreq.exe` auf dem fehlerhaften System kompilieren und ausführen, um zu bestimmen, ob bei **vsreq** und IBM Spectrum Protect dasselbe Problem auftritt. Wenn mit **vsreq** dasselbe Problem wie bei IBM Spectrum Protect reproduziert werden kann, kann die Ausgabe von **vsreq** dem Microsoft Support zur Verfügung gestellt werden, um Sie bei der Diagnose des VSS-Problems zu unterstützen.

In einigen Fällen stellt Microsoft ein E/A-Subsystemanalysetool („yapt") zum Zusammenstellen von E/A-Leistungsdaten für die Analyse bereit. Als Alternative zu **vsreq** steht außerdem das Tool **vshadow** zur Verfügung.

IBM Spectrum Protect-Interaktion mit VSS und Ntbackup.exe-Interaktion mit VSS vergleichen

Windows

Bei der Verwendung der ausführbaren Datei `Ntbackup.exe` wird Volume Shadow Copy Service (VSS) nicht vollständig genutzt und die Datei kann nicht immer als Vergleichspunkt für die IBM Spectrum Protect-Interaktion mit VSS verwendet werden.

Ein bekannter Unterschied im VSS-Kontext zwischen `Ntbackup.exe` und IBM Spectrum Protect besteht darin, dass `Ntbackup.exe` VSS nicht zum Sichern von Active Directory (NTDS) verwendet. Obwohl `Ntbackup.exe` VSS nutzt, um eine Momentaufnahme zu erstellen, verwendet Ntbackup.exe weiterhin die traditionelle NTDS-Sicherungs-API, um Daten von der Platte zu lesen. IBM Spectrum Protect verwendet die VSS-Schnittstelle, um NTDS-Daten von der Platte zu lesen. Wenn ein Problem mit dem VSS-Writer vorliegt, der für NTDS verantwortlich ist, wird dieses Problem mit `Ntbackup.exe` nicht offensichtlich.

Geben Sie den Befehl **VSSADMIN LIST** aus, um den Status des VSS-Writers abzufragen, um sicherzustellen, dass sich VSS in einem stabilen Status oder im Bereitstatus befindet.

Befehle SHOW für den Client für Sichern/Archivieren

Befehle **SHOW** sind nicht unterstützte Diagnosebefehle, die verwendet werden, um Informationen zu speicherinternen Steuerstrukturen und andere Laufzeitattribute anzuzeigen. Die Befehle **SHOW** werden von der Entwicklung und dem Service nur als Diagnosetools verwendet. Für den Client für Sichern/Archivieren sind mehrere Befehle **SHOW** vorhanden.

Abhängig von den Informationen, die von einem Befehl **SHOW** angezeigt werden, kann es Instanzen geben, bei denen sich die Informationen ändern, oder kann es Fälle geben, in denen die Informationen zur Folge haben, dass die Ausführung der Anwendung (Client, Server oder Speicheragent) gestoppt wird. Die Befehle **SHOW** dürfen nur verwendet werden, wenn dies von der Entwicklung oder dem Service vorgeschlagen wird. Die Befehle **SHOW** in Tabelle Tabelle 3 sind nicht alle verfügbaren Befehle **SHOW**.

Tabelle 3. Befehle SHOW für den Client für Sichern/Archivieren

Befehl SHOW	Beschreibung	Informationen
CLUSTER	Zeigt Informationen zu den Plattenzuordnungen in einem Microsoft-Cluster an.	Nützlich für das Anzeigen von Informationen zur Plattenzuordnung (Konfiguration) in einer Microsoft-Clusterumgebung.
DOMAIN	Zeigt Informationen zu den konfigurierten Domänen an, die für die Teilsicherungsverarbeitung verwendet werden.	Nützlich für das Anzeigen und Zusammenfassen der Clientoptionen `DOMAIN`, `DOMAIN.IMAGE` und `DOMAIN.NAS`.
OPTIONS	Zeigt die Clientoptionen an.	Nützlich für die Bestimmung der Einstellungen von Clientoptionen.
OPTTABLE	Zeigt Informationen zu Optionen an, die vom Server verwaltet werden, im Vergleich zu Optionen, die durch die Clientoptionsdatei verwaltet werden.	Der Client kann seine Optionseinstellungen entweder aus der Clientoptionsdatei oder vom Server erhalten. Um die Option vom Server zu erhalten, muss eine Clientoptionsgruppe mit dem Befehl **DEFINECLOPTSET** definiert werden. Dieser Befehl hilft Ihnen bei der Bestimmung, ob der Client eine in der Optionsdatei konfigurierte Option oder eine in der Clientoptionsgruppe auf dem Server konfigurierte Option verwendet.
PLUGINS	Zeigt Informationen zu installierten Plug-ins für diesen Client an.	Der Client verwendet Plug-ins, um zusätzliche Funktionen, wie z. B. Imagesicherung, bereitzustellen. Dieser Befehl **SHOW** zeigt die Plug-ins an, die für diesen Client installiert sind, und auch Attribute der verschiedenen Plug-ins, wie z. B. ihre Version, ihren Typ und ihre Position.

Tabelle 3. Befehle SHOW für den Client für Sichern/Archivieren (Forts.)

Befehl SHOW	Beschreibung	Informationen
SESSION	Zeigt die Funktionalität an, über die dieser Client für diese Verbindung zum Server verfügt.	Der Client und der Server melden und vereinbaren die Funktionalität, die jeder hat, wenn eine Sitzung zwischen einem Client und einem Server gestartet wird. Mit diesem Befehl **SHOW** wird die Funktionalität zurückgemeldet, die für diesen Server und Client verfügbar ist.
SYSTEMSTATE	Zeigt für Windows-Clients die **SYSTEM STATE**-Daten an, die auf diesem Client verfügbar sind.	Mit dem Befehl **SHOW** SYSTEMSTATE können die **SYSTEM STATE**-Dateien, die auf diesem Windows-System installiert sind, sowie die Dateien, für die eine Sicherung möglich ist, ermittelt werden.
TRACEFLAGS	Zeigt Informationen zu Traceklassen und zusammengefassten Traceklassen für diesen Client an.	Mit dem Befehl **SHOW** TRACEFLAGS können die Traceklassen und zusammengefassten Traceklassen bestimmt werden, die für diesen Client verwendet werden könnten.
VERSION	Zeigt die Version und das Erstellungsdatum für diesen Client an.	Mit dem Befehl **SHOW** VERSION kann bestimmt werden, welcher Client ausgeführt wird und wann er erstellt wurde.

Probleme bei der Wiederherstellung einzelner Microsoft SQL-Datenbanken aus der Sicherung einer virtuellen Maschine beheben

Windows

Mit IBM Spectrum Protect for Virtual Environments Data Protection for VMware können Sie einzelne Microsoft SQL-Datenbanken aus der Sicherung einer virtuellen Maschine wiederherstellen. Bei der Wiederherstellung einer Datenbank müssen möglicherweise häufig auftretende Probleme in Bezug auf einzelne SQL-Datenbanken behoben werden.

Wenn Sie den eigenständigen Anwendungsschutz für Microsoft SQL bei Data Protection for VMware verwenden, können Sie eine virtuelle Gastmaschine sichern, die als Host für eine Microsoft SQL Server-Anwendung dient. Falls Sie eine einzelne Microsoft SQL-Datenbank aus der Sicherung einer virtuellen Maschine zurückschreiben wollen, müssen Sie IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server verwenden.

In der folgenden Tabelle sind Lösungen für häufig auftretende Probleme aufgeführt, die bei dem Versuch entstehen können, einzelne Microsoft SQL-Datenbanken aus der Sicherung einer virtuellen Maschine wiederherzustellen.

Tabelle 4. Fehlerbehebungsinformationen für die Wiederherstellung einzelner Microsoft SQL-Datenbanken aus der Sicherung einer virtuellen Maschine

Fehler	Lösung oder Erläuterung
Sie können nicht mit Data Protection for SQL auf die Datenbanksicherungen zugreifen.	„Probleme beim Datenbankzugriff beheben"
Es werden ausschließlich inaktive Kopien von SQL-Datenbanken angezeigt, wenn Sie die Data Protection for SQL-GUI oder den Befehl **tdpsqlc** verwenden.	„Aktive Kopien von Microsoft SQL-Datenbanken anzeigen" auf Seite 53
SQL-Datenbanknamen, die Zeichen aus dem Doppelbytezeichensatz (DBCS) enthalten, können mit Data Protection for SQL nicht angezeigt werden.	„Microsoft SQL-Datenbanknamen mit DBCS-Zeichen" auf Seite 54
Sie haben während der Sicherung einer virtuellen Maschine den Anwendungsschutz verwendet und empfangen Warnungen sowie Fehlernachrichten.	„Maßnahmen bei Nachrichten für Sicherungen virtueller Maschinen mit Anwendungsschutz" auf Seite 54
Sie wollen ermitteln, welche SQL-Datenbanken sich zum Zeitpunkt der Sicherung einer virtuellen Maschine auf der virtuellen Gastmaschine befanden.	„VSS-XML-Manifestdateien speichern" auf Seite 55
Sie wollen den Status von VSS-Ausgabeprogrammen in der virtuellen Gastmaschine anzeigen.	„Potenziellen Fehlschlag der Sicherung einer virtuellen Maschine ermitteln" auf Seite 56

Probleme beim Datenbankzugriff beheben

Windows

Falls Sie eine virtuelle Gastmaschine gesichert haben, die als Host für eine Microsoft SQL Server-Anwendung dient, können Sie möglicherweise nicht mit Data Protection for SQL auf die Datenbanken zugreifen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Probleme mit dem Datenbankzugriff zu beheben:

1. Überprüfen Sie, ob der Anwendungsschutz verwendet wurde, als Sie die Sicherung der virtuellen Maschine erstellt haben:
   a. Geben Sie im Fenster mit Eingabeaufforderung den folgenden Befehl für den Client für Sichern/Archivieren aus, um die Liste mit den erfolgreichen Sicherungen virtueller Maschinen auf dem Server anzuzeigen:

      ```
      dsmc -node=Datencenterknoten query vm VM-Name -detail
      ```

      Hierbei steht *Datencenterknoten* für den Namen des virtuellen Knotens, der die Daten im Datencenter enthält, und *VM-Name* für den Namen der virtuellen Maschine, die Sie gesichert haben.
   b. Prüfen Sie, ob die Ausgabe dieses Befehls die folgenden Ausgabefelder enthält.

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

Falls die Befehlsausgabe diese Ausgabefelder nicht enthält oder im zweiten Feld nicht der Text `database-level recovery` angegeben ist, führen Sie die folgenden Schritte aus:

1) Stellen Sie sicher, dass der Client für Sichern/Archivieren Version 7.1 oder höher auf dem Knoten der Einheit zum Versetzen von Daten installiert ist und dass die Clientoptionsdatei die Option `include.vmtsmvss` *VM-Name* enthält.
2) Sichern Sie die virtuelle Gastmaschine erneut.

2. Stellen Sie sicher, dass der Computername der virtuellen Gastmaschine nach der Sicherung der virtuellen Maschine nicht geändert wurde.
3. Stellen Sie sicher, dass der DSMAGENT-Gastknoten auf die Sicherungen virtueller Maschinen des Datencenterknotens zugreifen kann.
   a. Geben Sie den folgenden Befehl aus, um sicherzustellen, dass der Clientknoten Zugriff auf Sicherungsversionen der virtuellen Maschine auf dem Server hat:

      ```
      dsmc –node=Datencenterknoten query access
      ```

      Hierbei steht *Datencenterknoten* für den Namen des virtuellen Knotens, der die Daten im Datencenter enthält.
   b. Prüfen Sie, ob die Befehlsausgabe die folgenden Felder enthält:

      ```
      Type     Node            User   Path
      ----     ----------------------------------------
      Backup   DSMAGENT-Knoten  *      \VMFULL-VM-Name\*\*
      ```

      Falls die Ausgabe diese Informationen nicht enthält, führen Sie den Befehl **set access** auf dem Knoten der Einheit zum Versetzen von Daten erneut aus, damit der DSMAGENT-Knoten Zugriff auf die Sicherungen der virtuellen Gastmaschine erhält. Geben Sie beispielsweise den folgenden Befehl aus:

      ```
      dsmc set access backup –type=vm DSMAGENT-Knoten VM-Name
      ```

      Hierbei steht *DSMAGENT-Knoten* für den Knotennamen des Clients für Sichern/Archivieren in der virtuellen Gastmaschine und *VM-Name* für den Namen der virtuellen Maschine, die Sie gesichert haben.

Nächste Schritte

Greifen Sie erneut mit Data Protection for SQL auf die einzelnen Datenbanken zu.

Aktive Kopien von Microsoft SQL-Datenbanken anzeigen

Windows

Damit die aktiven Kopien von Microsoft SQL-Datenbanken mit Data Protection for SQL angezeigt werden können, müssen Sie alle erstmaligen Sicherungen und nachfolgenden Teilsicherungen der SQL-Datenbanken unter Verwendung von Data Protection for VMware mit Anwendungsschutz ausführen.

Falls Sie für die erstmalige Sicherung von Microsoft SQL-Datenbanken den Anwendungsschutz verwendet haben, dies jedoch bei den nachfolgenden Teilsicherungen nicht der Fall war, gibt es keine gültigen aktiven Sicherungen, die für Zurückschreibungsoperationen von einzelnen SQL-Datenbanken verwendet werden können. Data Protection for SQL untersucht die Sicherung der virtuellen Maschine und kann nur diejenigen SQL-Datenbanken aus den Sicherungen virtueller Maschinen anzeigen, die erfolgreich mit Anwendungsschutz gesichert wurden.

Achten Sie darauf, den Anwendungsschutz bei der erstmaligen Sicherung und bei allen nachfolgenden Teilsicherungen der virtuellen Maschine zu aktivieren, auf der sich die Microsoft SQL-Anwendung befindet. Dieses Verfahren stellt sicher, dass die aktiven Kopien von SQL-Datenbanken, die Sie von einer virtuellen Maschine gesichert haben, von Data Protection for SQL angezeigt werden können.

Microsoft SQL-Datenbanknamen mit DBCS-Zeichen

Windows

Während Data Protection for VMware für Unicode aktiviert ist und Microsoft SQL-Datenbanken sichern kann, deren Namen Zeichen des Doppelbytezeichensatzes (DBCS) enthalten, ist Data Protection for SQL nicht für Unicode aktiviert. Data Protection for SQL kann daher nicht zum Zurückschreiben von Datenbanken mit DBCS-Zeichen im Namen aus einer virtuellen Maschine verwendet werden, die mit Anwendungsschutz gesichert wurde.

Um die Sicherung einer virtuellen Maschine zurückzuschreiben, die SQL-Datenbanken mit DBCS-Zeichen im Namen enthält, müssen Sie die gesamte Sicherung der virtuellen Maschine mit Data Protection for VMware zurückschreiben.

Maßnahmen bei Nachrichten für Sicherungen virtueller Maschinen mit Anwendungsschutz

Windows

Möglicherweise erhalten Sie bei Sicherungsoperationen für die virtuelle Maschine Warnungen oder Fehlernachrichten, wenn Sie den Anwendungsschutz verwenden.

Die folgenden Nachrichten werden unter Umständen angezeigt. Führen Sie in einem solchen Fall die folgenden Aktionen aus:

ANS2196W Eine inkompatible Plattenkonfiguration wird erkannt. Eine einzelne SQL-Datenbankzurückschreibung der Datenbank '*Datenbankname*' wird nicht unterstützt.

Bei einer Wiederherstellung einzelner SQL-Datenbanken können Sie lediglich Microsoft SQL-Datenbanken verwenden, die sich auf Basisplatten mit einer Master-Bootsatz-Partitionierung (MBR-Partitionierung) befinden. Diese Warnung gibt an, dass eine oder mehrere SQL-Datenbanken eine nicht unterstützte Plattenkonfiguration aufweisen.

ANS2330E Die Blockierung der VSS-Ausgabeprogramme konnte nicht aufgehoben werden, weil die Momentaufnahmezeit das zulässige Zeitlimit von 10 Sekunden überschritten hat.

Ermitteln Sie durch die folgenden Aktionen, ob ein Fehler vorliegt:

1. Erstellen Sie mit dem vSphere-Client die Momentaufnahme einer virtuellen Maschine im Quiescemodus. Falls diese Aktion erfolgreich ist, fahren Sie mit dem nächsten Schritt fort.

   Ist diese Aktion nicht erfolgreich, hängt das Problem wahrscheinlich mit VMware zusammen. Sie müssen sich bezüglich des Problems mit dem VMware Support in Verbindung setzen.
2. Sichern Sie die virtuelle Maschine ohne Anwendungsschutz:
   a. Inaktivieren Sie den Anwendungsschutz, indem Sie die Option `INCLUDE.VMTSMVSS` *VM-Name* aus der Clientoptionsdatei entfernen.

b. Führen Sie den folgenden Befehl im Fenster mit Eingabeaufforderung aus, um eine Sicherung für die virtuelle Maschine durchzuführen:

   ```
   dsmc backup vm VM-Name -vmbackuptype=fullvm
   ```

   Hierbei steht *VM-Name* für den Namen der virtuellen Maschine, die Sie sichern wollen.

Die bis jetzt von Ihnen ausgeführten Schritte können Sie bei der weitergehenden Diagnose und der Behebung des Problems unterstützen. Falls dieser Schritt jedoch nicht erfolgreich ist, liegt ein Problem mit der virtuellen Windows-Gastmaschine oder mit dem Client für Sichern/Archivieren auf dem Knoten der Einheit zum Versetzen von Daten vor. Möglicherweise müssen Sie nach weiteren Supportinformationen für IBM Spectrum Protect im IBM Support Portal for IBM Spectrum Protect suchen.

VSS-XML-Manifestdateien speichern

Windows

Wenn Sie VSS-XML-Manifestdateien speichern, können Sie einfacher ermitteln, welche Microsoft SQL-Datenbanken zum Zeitpunkt der Sicherung auf der virtuellen Gastmaschine vorhanden waren.

Informationen zu diesem Vorgang

VSS-XML-Manifestdateien enthalten VSS-Writerinformationen, die während einer Sicherungsoperation für die virtuelle Maschine generiert werden. Die VSS-XML-Manifestdateien werden für VSS-Zurückschreibungsoperationen von ausgewählten Microsoft SQL-Datenbanken benötigt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die VSS-XML-Manifestdateien auf dem Knoten der Einheit zum Versetzen von Daten zu speichern:

1. Fügen Sie die folgende Anweisung zur Clientoptionsdatei hinzu:

   ```
   testflag VMBACKup_SAVE_LOCAL
   ```

2. Starten Sie die Sicherung einer virtuellen Maschine mit Anwendungsschutz auf der virtuellen Gastmaschine, die als Host für die SQL Server-Anwendung dient.

   Nach Abschluss der Sicherungsoperation für die virtuelle Maschine werden die VSS-XML-Manifestdateien an der folgenden Position auf dem Knoten der Einheit zum Versetzen von Daten gespeichert:

   ```
   C:\mnt\tsmvmbackup\fullvm\vmtsmvss\VM-Name
   ```

   Hierbei steht *VM-Name* für den Namen der virtuellen Maschine, die gesichert wurde.

3. Zeigen Sie die Liste der SQL-Datenbanken an, die sich zum Zeitpunkt der Sicherung auf der virtuellen Gastmaschine befunden haben, indem Sie die Datei `sqldbinfo.xml` mit einem Texteditor öffnen. Prüfen Sie, ob die Datei `sqldbinfo.xml` vollständige Informationen zu den gesicherten SQL-Datenbanken enthält.

Potenziellen Fehlschlag der Sicherung einer virtuellen Maschine ermitteln

Windows

Indem Sie den Status der VSS-Ausgabeprogramme in einer virtuellen Gastmaschine überprüfen, können Sie ermitteln, ob die Sicherung einer virtuellen Maschine mit Anwendungsschutz fehlschlagen könnte.

Informationen zu diesem Vorgang

Zeigen Sie den Status der VSS-Ausgabeprogramme mit dem Befehl **vssadmin list writers** an. Dieser Befehl listet alle auf der virtuellen Gastmaschine verfügbaren Ausgabeprogramme inklusive ihres Status auf. Falls der Status von einem oder mehreren VSS-Ausgabeprogrammen nicht stabil ist, schlägt die Sicherung einer virtuellen Maschine mit Anwendungsschutz fehl.

Vorgehensweise

Geben Sie im Fenster mit Eingabeaufforderung den folgenden Befehl aus:

```
vssadmin list writers
```

Das folgende Beispiel zeigt die Befehlsausgabe:

```
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
```

Der Status des VSS-Ausgabeprogramms ist im Feld `State` angegeben.

Kapitel 3. Probleme mit dem IBM Spectrum Protect-Server beheben

Wenn Sie mit IBM Spectrum Protect arbeiten, können bestimmte Probleme mit dem Server auftreten. Die Diagnoseschritte, die Sie für den Server ausführen können, reichen von einfachen Aktionen, wie z. B. Neustart des Servers, bis hin zu komplexen Prozeduren.

Die folgende Liste enthält einige Aktionen, die Sie ausführen können, um Serverprobleme zu diagnostizieren:

- Problem reproduzieren
- Serveraktivitätenprotokoll und andere Protokolle überprüfen
- Fehlerprotokolle überprüfen, die sich auf das Lesen von einer Einheit oder das Schreiben auf eine Einheit beziehen
- Serveroptionen ändern
- Zeitplanungsservices stoppen und starten
- Datenbank oder Speicherpool abfragen
- Trace für Traceklasse UNICODE erstellen

Fehler reproduzieren

Kann der Fehler einfach oder konsistent reproduziert werden, reproduzieren Sie den Fehler, um die Ursache auf eine bestimmte Folge von Ereignissen einzugrenzen.

Viele Fehler sind das Ergebnis einer Kombination von Ereignissen. Beispiel: Die Verfallsverarbeitung wird zusammen mit nächtlich geplanten Sicherungen für 20 Clients ausgeführt. In einigen Fällen können Sie das erneute Auftreten des Fehlers verhindern, indem Sie den zeitlichen Ablauf oder die Reihenfolge der Implementierung von Ereignissen ändern. Eine Möglichkeit, den zeitlichen Ablauf zu ändern, ist die Ausführung der Verfallsverarbeitung zu einer Zeit, zu der die nächtlich geplanten Sicherungen für 20 Clients nicht ausgeführt werden.

Serveraktivitätenprotokolldatei und andere Protokolldateien überprüfen

Überprüfen Sie die Serveraktivitätenprotokolldatei auf Nachrichten, die 30 Minuten vor und 30 Minuten nach dem Fehler empfangen wurden.

Um die Nachrichten im Serveraktivitätenprotokoll zu überprüfen, geben Sie den Befehl **QUERY ACTLOG** aus. Oft können andere Nachrichten weitere Informationen zur Ursache und Behebung des Fehlers bereitstellen.

Liste zusätzlicher Protokolldateien

Der IBM Software Support fordert Sie möglicherweise auf, die folgenden Protokolldateien zu senden.

- Web-Server-Protokolldateien:
  - `console.log`
  - `messages.log`
- FFDC-Protokolldateien (FFDC - Erfassung von Fehlerdaten beim ersten Auftreten):

- exception_summary_*Datum_Zeit*.log
- ffdc_*Datum_Zeit*.log

Speicherposition von Protokolldateien

- Die Web-Server-Protokolldateien befinden sich im folgenden Verzeichnis:

  AIX Linux *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer/logs

  Windows *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer\logs

  Dabei steht *Installationsverzeichnis* für das Verzeichnis, in dem IBM Spectrum Protect installiert ist. Beispiel:

  AIX Linux /opt/tivoli/tsm

  Windows c:\Programme\Tivoli\TSM
- Die FFDC-Protokolldateien befinden sich an derselben Speicherposition, aber im Unterverzeichnis ffdc.

Systemfehlerprotokolldateien auf Einheitenfehler überprüfen

Handelt es sich um einen Fehler, der beim Lesen von Daten von einer Einheit oder beim Schreiben von Daten auf eine Einheit auftritt, zeichnen viele Systeme und Einheiten Informationen in einem Systemfehlerprotokoll auf.

Wenn eine Einheit oder ein Datenträger, die bzw. der von IBM Spectrum Protect verwendet wird, einen Fehler an das Systemfehlerprotokoll zurückmeldet, handelt es sich wahrscheinlich um einen Einheitenfehler. Die im Systemfehlerprotokoll aufgezeichneten Fehlernachrichten stellen möglicherweise genügend Informationen bereit, um den Fehler zu beheben.

Nachfolgend sind einige Beispiele für Systemfehlerprotokolle aufgeführt:

- errpt für AIX
- Ereignisprotokoll für Windows

Serveroptionen oder -einstellungen zurücksetzen

Wurden Konfigurationsänderungen am Server vorgenommen, versuchen Sie, die Einstellungen auf ihre ursprünglichen Werte zurückzusetzen, und wiederholen Sie die fehlgeschlagene Operation.

Ist die Operation erfolgreich, versuchen Sie, jeweils eine Änderung vorzunehmen, und wiederholen Sie die Operation, bis die Attributänderung, die den Fehler verursacht hat, identifiziert wurde.

Änderungen an Optionen in der Serveroptionsdatei oder Konfigurationsänderungen, die mit dem Befehl **SET** oder **UPDATE** am Server vorgenommen wurden, können Fehler bei Operationen verursachen, die zuvor erfolgreich ausgeführt wurden. Änderungen auf dem Server an Einheitenklassen, Speicherpools und Maßnahmen können ebenfalls zu Fehlern bei Operationen führen, die zuvor erfolgreich ausgeführt wurden.

Zeitplanungsservice erneut starten

Geplante Clientoperationen werden durch die Zeitplandefinitionen auf dem Server sowie durch den Zeitplanungsservice (dsmsched), der auf dem Client-Computer selbst ausgeführt wird, beeinflusst.

Starten Sie den Zeitplanungsservice auf dem Client erneut, wenn sich ein Zeitplan auf dem Server ändert.

Wichtig: Wird der Zeitplanungsservice durch den Clientakzeptor gesteuert, stoppen Sie nur den Clientakzeptor und starten Sie ihn erneut.

Probleme mit Serverspeicherbereich beheben

Die primäre Funktion des IBM Spectrum Protect-Servers ist das Speichern von Daten. Wenn der Server über keinen Speicherbereich mehr in der Datenbank oder den Speicherpools verfügt, können Operationen fehlschlagen.

Um zu bestimmen, ob die Datenbank über keinen Speicherbereich verfügt, geben Sie den Befehl **QUERY DB** aus. Wenn die prozentuale Auslastung (belegter Speicherbereich) bei 100 % liegt, definieren Sie mehr Speicherbereich. Verfügt die Datenbank über keinen Speicherbereich mehr, werden normalerweise andere Servernachrichten ausgegeben.

Um zu bestimmen, ob ein Speicherpool über keinen Speicherbereich verfügt, geben Sie den Befehl **QUERY STGPOOL** aus. Wenn die prozentuale Auslastung bei 100 % liegt, stellen Sie mehr Speicherbereich zur Verfügung. Um einem Plattenspeicherpool (DISK) mehr Speicherbereich hinzuzufügen, ordnen Sie einen oder mehr neue Speicherpools zu und definieren Sie diese Speicherpools mit dem Befehl **DEFINE VOLUME** für den Server. Sie können IBM Spectrum Protect so konfigurieren, dass automatisch Speicherbereich für DISK- und FILE-Speicherpools zugeordnet wird, indem Sie den Befehl **DEFINE SPACETRIGGER** verwenden.

Um einem Speicherpool für sequenzielle Datenträger mehr Speicherbereich hinzuzufügen, überprüfen Sie das Bandarchiv und bestimmen Sie, ob weitere Arbeitsbänder hinzugefügt werden können. Ist dies der Fall, fügen Sie dem Archiv die zusätzlichen Arbeitsdatenträger hinzu und aktualisieren Sie den Parameter **MAXSCR** für den Speicherpool, indem Sie den Befehl **UPDATE STGPOOL** ausgeben.

Zusätzlichen Serverspeicher zuordnen

Ordnen Sie mehr Speicher auf dem Server zu, wenn es Anzeichen dafür gibt, dass Ihr Server über wenig Speicherressourcen verfügt. Die Dokumentation zu Ihrem Betriebssystem enthält Informationen zum Hinzufügen von Speicher.

Tipp: Die Speichermenge, die von DB2 verwendet wird, kann zu Berichten beitragen, die anzeigen, dass das Betriebssystem über keinen Speicher verfügt. Sie können die von DB2 verwendete Speichermenge begrenzen, indem Sie die Option `DBMEMPERCENT` einschließen. Die Option `DBMEMPERCENT` gibt den Prozentsatz des virtuellen Adressraums an, der den Datenbankmanagerprozessen zugeordnet ist.

Führen Sie die folgenden Aktionen aus, um zusätzliche Speicherressourcen für den Server zuzuordnen:

- AIX Stellen Sie sicher, dass genügend Paging-Bereich vorhanden ist. Sie können auch SMIT (System Management Interface Tool) verwenden, um zu bestimmen, ob die Anzahl der Anwendungen den Speichermangel verursacht.
- Windows Die bevorzugte Methode zur Behebung des Speichermangels ist das Hinzufügen physischen Speichers zum System. Andernfalls erhöhen Sie über die Systemsteuerung den virtuellen Speicher, indem Sie das Systemapplet ausführen und die Paging-Dateigesamtgröße erhöhen.

Serverinstanz für die Verwendung von gemeinsam genutztem Speicher konfigurieren

Wenn Sie eine Serverinstanz für die Verwendung von gemeinsam genutztem Speicher konfigurieren, kann dies die Auflösung von langsamen Datenbanksicherungen fördern, die aufgrund von Loopbackproblemen bei TCP (Transmission Control Protocol) auftreten.

Informationen zu diesem Vorgang

In der folgenden Prozedur müssen Sie die Konfiguration des Datenbanksicherungsknotens aktualisieren, damit der Server gemeinsam genutzten Speicher verwenden kann.

- AIX Linux *Verzeichnis_server_bin*/dbbkapi/dsm.sys
- Windows *Serverinstanzverzeichnis*\tsmdbmgr.opt

Vorgehensweise

1. Stellen Sie sicher, dass die Serveroptionsdatei `dsmserv.opt` die folgenden Zeilen enthält:

   ```
   COMMMethod SHAREdmem
   SHMPort         1510
   ```

2. AIX Linux Ändern Sie die Zeilengruppe für den Datenbanksicherungsknoten in der Systemoptionsdatei `dsm.sys` für die Client-API.
   - Entfernen Sie die folgenden Zeilen aus der Zeilengruppe:

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

   - Fügen Sie die folgenden Zeilen zur Zeilengruppe hinzu:

     ```
     COMMMethod SHAREdmem
     SHMPort 1510
     ```

3. Windows Ändern Sie die Zeilengruppe für den Datenbanksicherungsknoten in der Systemoptionsdatei `tsmdbmgr.opt` für die Client-API.
   - Entfernen Sie die folgenden Zeilen aus der Datei `tsmdbmgr.opt`:

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

   - Fügen Sie die folgenden Zeilen zur Datei `tsmdbmgr.opt` hinzu:

     ```
     COMMMethod SHAREdmem
     SHMPort 1510
     ```

Kopienhäufigkeit ändern

Die IBM Spectrum Protect-Servermaßnahme verlangt, dass die Kopienhäufigkeit für Teilsicherungen einen Wert ungleich null hat.

Das Attribut für die Kopienhäufigkeit der aktuellen *Kopiengruppen*verwaltungsklasse für die angegebene Datei bestimmt die Mindestanzahl der Tage, die zwischen aufeinanderfolgenden Teilsicherungen vergehen müssen. Soll eine Teilsicherung für eine Datei ausgeführt werden und sind für diese Anzahl mehr als 0 Tage angegeben, wird die Datei nicht an den Server gesendet, selbst wenn sich die Datei geändert hat.

Sie können eine Reihe von Schritten ausführen, um diesen Fehler zu korrigieren:

- Wenden Sie sich an den Serveradministrator, um das Attribut für die Kopienhäufigkeit zu ändern.
- Führen Sie eine selektive Sicherung der Datei aus. Beispiel: `DSMC SELECTIVE C:\FILE.TXT`

Sie können den Befehl **QUERY COPYGROUP** ausgeben, um die Einstellung des Parameters für die Kopienhäufigkeit zu bestimmen:

```
tsm: WINBETA>q copygroup standard active f=d
Name der Maßnahmendomäne: STANDARD
 ...
Kopienhäufigkeit: 1
 ...
```

Fehler bei RELABEL-Operation beheben

Wird eine RELABEL-Operation ausgeführt, wenn alle Laufwerke aktiv sind, kann der Zieldatenträger nicht mit einem neuen Kennsatz versehen werden, da er kein Laufwerk anfordern kann. Aktive Laufwerke sind Laufwerke, die für regelmäßige Operationen, wie z. B. Sicherung, Zurückschreibung, Umlagerung und Wiederherstellung, im Gebrauch sind.

Wenn ein RELABEL-Fehler auftritt, werden die folgenden Beispielinformationen generiert:

```
ANR0984I Prozess 25 für RELABEL im BACKGROUND um 22:10:36 gestartet.
ANR8799I RELABEL: Operation für Kassettenarchiv IBMVTL als Prozess 25 gestartet.
ANR1341I Arbeitsdatenträger 007403 wurde aus dem Speicherpool VTLPOOL gelöscht.
ANR8847E Keine Laufwerke mit Einheitentyp LTO sind derzeit im Kassettenarchiv
IBMVTL verfügbar.
ANR8801I LABEL LIBVOLUME: Prozess 25 für Kassettenarchiv IBMVTL beendet;
0 Datenträger mit Kennsatz versehen, 0 Datenträger zurückgestellt.
ANR0985I Prozess 25 für RELABEL, der im BACKGROUND ausgeführt wird, mit
Beendigungsstatus SUCCESS um 22:10:36 beendet.
```

Führen Sie die folgenden Schritte aus, um einen RELABEL-Fehler zu beheben:

1. Stellen Sie sicher, dass ein Laufwerk für die RELABEL-Operation verfügbar ist, und versehen Sie einen Zieldatenträger mit einem neuen Kennsatz.
2. Aktualisieren Sie die Einheitenklassen, die auf das Kassettenarchiv verweisen. Aktualisieren Sie die Einheitenklassen mit einem Wert für den Parameter **MOUNTLIMIT**, der kleiner als die Gesamtzahl der verfügbaren Laufwerke ist.

   Wenn eine RELABEL-Operation kein Laufwerk anfordern kann oder einen Datenträger nicht mit einem neuen Kennsatz versehen kann, versucht IBM Spectrum Protect, den Datenträger bei jeder zukünftigen RELABEL-Operation mit einem neuen Kennsatz zu versehen.

Wenn die RELABEL-Operation fehlschlägt, geben Sie den Befehl **LABEL LIBVOLUME** für alle Datenträger aus, die in IBM Spectrum Protect entnommen, aber nicht mit einem neuen Kennsatz versehen sind. Schließen Sie die folgenden Parameter in den Befehl **LABEL LIBVOLUME** ein:

```
SEARCH=YES LABELSOURCE=BARCODE OVERWRITE=YES CHECKIN=SCRATCH
```

Übertragungsfehler bei der Importverarbeitung vermeiden

Im Aktivitätenprotokoll des Zielservers werden Übertragungsfehler gemeldet, wenn Sie den Importprozess vom Zielserver aus abbrechen.

Falls Sie den Importprozess vom Zielserver aus abbrechen, geben Übertragungsfehlernachrichten im Aktivitätenprotokoll den Knotennamen an, der die Exportoperation vom Quellenserver aus gestartet hat. Die folgenden Nachrichten können beispielsweise im Serveraktivitätenprotokoll angegeben sein:

```
ANR0440W Protokollfehler in Sitzung 2 für Knoten ADMIN
ANR3174E Übertragungsfehler mit verwaltetem Server ADMIN.
ANR0484W Sitzung 2 für Knoten ADMIN beendet - fehlerhaftes Protokoll erkannt.
```

Sie können die Übertragungsfehlernachrichten im Aktivitätenprotokoll des Zielservers, die sich auf die Importverarbeitung beziehen, ignorieren. Alternativ können Sie auch die Importverarbeitung vom Quellenserver aus abbrechen. In diesem Fall werden weder auf dem Quellen- noch auf dem Zielserver Übertragungsfehlernachrichten gemeldet.

Selbst signiertes Zertifikat zum Schlüsselspeicher hinzufügen

Sie können eine sichere Kommunikation konfigurieren, indem Sie ein selbst signiertes Zertifikat mit Ihrem Objektspeichersystem verwenden. In dieser Situation verwendet IBM Spectrum Protect `HTTPS` anstelle von `HTTP` bei der Kommunikation mit dem Objektspeichersystem. Die folgenden Schritte stellen eine Methode für das Importieren von Zertifikaten bereit.

Informationen zu diesem Vorgang

Verwenden Sie einen Web-Browser, um eine Kopie des Zertifikats abzurufen, das vom Objektspeichersystem verwendet wird. Die folgenden Schritte gelten für Firefox, aber andere Browser stellen ähnliche Funktionen bereit. Lesen Sie die Anweisungen Ihres bevorzugten Browsers zum Exportieren von Zertifikaten.

Vorgehensweise

1. Rufen Sie das Zertifikat ab, das vom OpenStack Swift-Server oder von IBM Cloud Object Storage verwendet wird.
   a. Geben Sie die URL Ihres Objektspeichersystems in die Adressleiste des Browsers ein und drücken Sie die **Eingabetaste**. Verwenden Sie die Keystone-Server-URL für OpenStack oder die Accesser-Knoten-URL für IBM Cloud Object Storage.

      Tipp: Wenn Sie IBM Cloud Object Storage als Objektspeichersystem verwenden, melden Sie sich bei IBM Cloud Object Storage an und klicken Sie auf die Registerkarte **Security**. Klicken Sie im Abschnitt **dsNet Fingerprint** auf **dsNet certificate authority** und kopieren Sie die Zertifikatsinformationen in eine Zertifikatsdatei für Teil 2.
   b. Akzeptieren Sie alle vom Browser angezeigten Warnungen.
   c. Klicken Sie auf das Sperrsymbol in der Adressleiste des Browsers.

d. Wählen Sie **Weitere Informationen** im Popup-Fenster aus.
e. Wählen Sie **Zertifikat anzeigen** im Fenster **Seiteninformation** aus.
f. Klicken Sie auf der Seite **Zertifikat-Ansicht** auf die Registerkarte **Details** und wählen Sie dann **Exportieren** aus.
g. Speichern Sie die exportierte Datei an der gewünschten Position.

2. Fügen Sie das Zertifikat dem Java-Standardschlüsselspeicher hinzu.

   In den folgenden Schritten wird vorausgesetzt, dass Ihre Clientknoten und Ihr Server unter Linux ausgeführt werden. Da jeder IBM Cloud Object Storage-Accesser standardmäßig sein eigenes Zertifikat hat, fügen Sie das Zertifikat für jeden Accesser dem Schlüsselspeicher hinzu und verwenden Sie einen unterschiedlichen Aliasnamen für jedes Zertifikat.

   a. Öffnen Sie ein Terminal und wechseln Sie in das Verzeichnis `jre/bin`.

      Die Standardinstallationsposition ist `/opt/tivoli/tsm/jre/bin`.

   b. Erstellen Sie eine Sicherungskopie der Java-Datei `cacerts`, indem Sie den folgenden Befehl ausführen: `cp ../lib/security/cacerts ../lib/security/cacerts.original`.

      Auf einem Windows-System befindet sich der Java-Schlüsselspeicher `cacerts` an der Position *`Installationsverzeichnis`*`\jre\lib\security\`, und die Position von keytool lautet *`Installationsverzeichnis`*`\jre\bin\`.

   c. Importieren Sie das gespeicherte Zertifikat aus der vorherigen Prozedur, indem Sie den folgenden Befehl ausführen: `./keytool -import -keystore ../lib/security/cacerts -alias` *`Aliasname`* `-file` *`Ihre_Datei`*.

      Dabei sind: *`Aliasname`* ist ein eindeutiger Aliasname für dieses Zertifikat im Schlüsselspeicher. Dieser Aliasname ist wichtig, wenn Sie mehrere Zertifikate haben. *`Ihre_Datei`* ist der Pfad und Dateiname des Zertifikats aus dem ersten Schritt dieser Anweisungen.

   d. Wenn Sie nach dem Kennwort gefragt werden, geben Sie *changeit* ein. Wenn Sie Ihr Standardkennwort geändert haben, geben Sie das aktuelle Kennwort ein.

   e. Wenn Sie gefragt werden, ob dieses Zertifikat vertrauenswürdig ist, geben Sie *Ja* ein.

      Die folgende Nachricht wird angezeigt, wenn das Zertifikat erfolgreich hinzugefügt wurde: `Zertifikat wurde dem Schlüsselspeicher hinzugefügt`. Die Standardzertifikate haben eine kurze Laufzeit. Wenn sie verfallen, können Sie möglicherweise nicht mehr auf den Objektspeicher zugreifen, bis Sie die Zertifikate aktualisieren. Sie können eigene Zertifikate erstellen und die Zertifikate verwenden, aber die Erstellung und Installation dieser Zertifikate auf Objektspeichersystemen liegt außerhalb des Geltungsbereichs dieses Dokuments.

   f. Starten Sie den IBM Spectrum Protect-Server erneut.

Feststellen, warum Summensätze für ein Clientsicherungsereignis fehlen

Wenn eine Kommunikationssitzung zwischen einem Client und einem Server abnormal beendet wird, werden die Summensätze für ein Clientsicherungsereignis möglicherweise mit Verzögerung der Serverdatenbank hinzugefügt.

Symptom

Nach Abschluss eines Clientsicherungsprozesses wird der Datensatz nicht sofort der Datenbank hinzugefügt. Es kann mehrere Stunden dauern, bis der Summensatz der Datenbank hinzugefügt wird.

Ursachen

Es kann mehrere Stunden dauern, bis die Summensätze der Serverdatenbank hinzugefügt werden, da eine Serversitzung warten muss, bis die Absturzbehandlung abgeschlossen ist. Eine Sitzung kann aus den folgenden Gründen abnormal beendet werden:

- Netzausfälle
- Sitzungszeitlimitüberschreitungen

Sitzungszeitlimitüberschreitungen können auftreten, wenn Sicherungsprozesse länger als erwartet dauern.

Problemlösung

1. Führen Sie die folgenden Aktionen aus, um festzustellen, warum Client/Server-Kommunikationssitzungen abnormal beendet wurden:
   a. Überprüfen Sie das Aktivitätenprotokoll durch Ausgabe des Befehls **QUERY ACTLOG**.
   b. Überprüfen Sie das Clientfehlerprotokoll `dsmerror.log` im Clientinstallationsverzeichnis.
   c. Falls Sie die Problemursache nicht durch Überprüfen der Protokollaktivität finden können, aktivieren Sie die Tracefunktion für den Client für Sichern/Archivieren.
2. Beheben Sie alle Kommunikationsprobleme. Sie können mit dem für das Netz zuständigen Team zusammenarbeiten, um Netzdaten zu erfassen und zu analysieren.

Zugehörige Verweise:

„Trace für Client für Sichern/Archivieren aktivieren” auf Seite 161

Probleme bei der Installation und der Durchführung eines Upgrades beheben

Zur Behebung von Installationsproblemen mit dem IBM Spectrum Protect-Server können die Überprüfung von Protokolldateien, die Neuinstallation des Servers oder verschiedene andere mögliche Optionen gehören.

Installationsprotokolldateien

Falls während des Installationsprozesses Fehler auftreten, werden diese Fehler in Protokolldateien aufgezeichnet.

Sie können die Installationsprotokolldateien anzeigen, indem Sie im Tool 'Installation Manager' auf **Datei** > **Protokoll anzeigen** klicken. Um diese Protokolldateien zu erfassen, klicken Sie im Tool 'Installation Manager' auf **Hilfe** > **Daten zur Fehleranalyse exportieren**.

Die Protokolldateien werden im IBM Installation Manager-Protokollverzeichnis gespeichert:

AIX Linux `/var/ibm/InstallationManager/logs`

Windows `C:\Programme\IBM\Installation Manager\logs`

Fehlgeschlagener Start des Installationsassistenten

IBM Installation Manager benötigt gtk-Bibliotheken, damit die grafische Benutzerschnittstelle (GUI) auf AIX-Systemen unterstützt wird. Falls diese Bibliotheken vor der Installation des IBM Spectrum Protect-Servers nicht installiert wurden, schlägt möglicherweise der Start der Installation fehl. Es wird eine Fehlernachricht über fehlende gtk-Bibliotheken ausgegeben.

Zugehörige Informationen:

IBM Spectrum Protect mithilfe des Installationsassistenten installieren

GSKit-Installationsfehler beheben

Wenn Sie die IBM Spectrum Protect-Installationssoftware verwenden, wird die korrekte Version von Global Security Kit (GSKit) automatisch installiert.

Falls die Umgebung der IBM Spectrum Protect-Serverinstanz nicht ordnungsgemäß konfiguriert ist, kann der Server die entsprechenden GSKit-Bibliotheken möglicherweise nicht laden. Der Konfigurationsassistent für die Serverinstanz hilft Ihnen bei der Vermeidung vieler Probleme, die beim manuellen Konfigurieren der Instanz auftreten können.

Windows Geben Sie den folgenden Befehl aus:

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

Dabei ist *X* das Systemlaufwerk. Die Umgebungsvariable PATH wird geändert, sodass sie auf das korrekte Verzeichnis verweist.

Linux Aktualisieren Sie `LD_LIBRARY_PATH` oder die Shell, indem Sie den folgenden Befehl ausgeben:

```
export LD_LIBRARY_PATH=plattformspezifisches-gskit-Bibliotheksverzeichnis:$LD_LIBRARY_PATH
```

Dabei ist *plattformspezifisches-gskit-Bibliotheksverzeichnis* eines der folgenden Verzeichnisse (entsprechend Ihrer Plattform):

- Linux `/usr/local/ibm/gsk8_64/lib64`

AIX Geben Sie bei AIX den folgenden Befehl aus:

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

AIX Linux Sie müssen die folgenden Dateien aktualisieren, um den Bibliothekspfad zu definieren, wenn DB2 oder der Server gestartet wird:

- *Instanzverzeichnis*`/sqllib/usercshrc`
- *Instanzverzeichnis*`/sqllib/userprofile`

Fügen Sie für die Datei *Instanzverzeichnis*`/sqllib/usercshrc` die folgenden Zeilen hinzu:

- AIX

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

- Linux

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

Fügen Sie für die Datei *Instanzverzeichnis*/sqllib/userprofile die folgenden Zeilen hinzu:

- 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
```

Überprüfen Sie die Bibliothekspfadeinstellungen und die GSKit-Version, indem Sie die folgenden Befehle ausgeben:

- AIX

```
echo $LIBPATH
gsk8capicmd_64 -version
```

- Linux

```
echo $LD_LIBRARY_PATH
gsk8ver_64
```

Ist die GSKit-Version nicht 8.0.14.28 oder höher, müssen Sie den Server erneut installieren. Die Neuinstallation stellt sicher, dass die richtige GSKit-Version verfügbar ist.

Keine Erstellung von Serverinstanzen bei Upgrade

Wenn keine Verbindung hergestellt werden kann, kann das Installationsprogramm Ihre IBM Spectrum Protect-Serverinstanzen nicht erneut erstellen. Sie müssen Ihre Serverinstanzen manuell erneut erstellen.

Informationen zu diesem Vorgang

Der Installationsassistent verwendet die folgenden Methoden, um eine Verbindung zum System herzustellen, um die Serverinstanzen erneut erstellen zu können:

- AIX Linux Secure Shell (SSH)
- Windows Windows Server Message Block (SMB)

Wenn Sie eine dieser Methoden für den Standardanschluss verwenden, darf der Anschluss nicht durch eine Firewall blockiert werden. Wenn er blockiert wird, führen Sie die folgenden Schritte aus, um ein manuelles Upgrade für die Serverinstanz durchzuführen. AIX Linux

Vorgehensweise

1. Schließen Sie den Installationsassistenten.
2. Führen Sie die folgenden Schritte für jede Serverinstanz aus:
   a. Nachdem das Upgrade abgeschlossen ist, geben Sie den folgenden Befehl aus, um die Instanz erneut zu erstellen:

      ```
      /opt/tivoli/tsm/db2/instance/db2icrt –u Instanzbenutzer Instanzname
      ```

   b. Erstellen Sie die Variablen in der Instanzdatei erneut. Geben Sie den Befehl **db2set -i** für jede Variable in der Instanzdatei aus. Legen Sie beispielsweise die Variable *DB2COMM* so fest, dass sie für die Instanz MYINST nur TCPIP angibt:

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

Geben Sie den Parameter **-all** an, um eine Liste aller definierten Variablen anzuzeigen, z. B. **db2set -all**.

c. Geben Sie den Befehl **db2stop** aus, um die Datenbankinstanz zu stoppen.

d. Verwenden Sie die Benutzer-ID, die Eigner der Serverinstanz ist, um den Befehl **db2start** zum Starten der Datenbankinstanz auszugeben.

e. Geben Sie die folgenden Befehle aus, um jede Datenbank zu katalogisieren und ein Upgrade für jede Datenbank durchzuführen:

```
db2 catalog db TSMDB1 on "Datenbankpfad"
db2 upgrade db TSMDB1
```

f. Geben Sie den Befehl **db2stop** aus.

g. Starten Sie den Server.

Problem mit einem gestoppten Deinstallationsprozess beheben

Ein abgelaufenes Kennwort für einen DB2-Instanzbenutzer kann dazu führen, dass der Deinstallationsprozess für IBM Spectrum Protect vor seiner Fertigstellung gestoppt wird.

Wenn das Kennwort für die DB2-Instanzbenutzer-ID abgelaufen ist, kann der Deinstallationsprozess nicht ausgeführt werden. Sie müssen sich mit der ID für die DB2-Instanz anmelden und das Kennwort zurücksetzen. Deinstallieren Sie dann IBM Spectrum Protect.

Kein Upgrade der Client-Software bei automatischer Clientimplementierung

Falls der Implementierungszeitplan ausgeführt wurde, für die Client-Software jedoch kein Upgrade auf die Zielversion erfolgt ist, überprüfen Sie die Protokolldateien auf dem Clientsystem.

Symptom

Nach Abschluss des Zeitplans für die automatische Implementierung ist für die Client-Software kein Upgrade auf die Zielversion erfolgt.

Ursache

Die folgenden Beispiele geben einige Ursachen für das nicht erfolgte Upgrade der Client-Software auf die Zielversion an.

- Im Clientdateisystem ist nicht genügend Speicherplatz für die Durchführung des Upgrades verfügbar.
- Netzprobleme haben verhindert, dass die Daten vom Server an das Clientsystem übertragen wurden.

Problemlösung

Sie können das Fehlschlagen des Client-Upgrades beheben, indem Sie die Protokoll- und Tracedateien auf dem Clientsystem prüfen. Der Deployment Manager schreibt Protokoll- und Tracedaten für eine Implementierungsoperation in das Clientdateisystem. Die Position der Protokolldateien ist in der Definition des Implementierungszeitplans auf dem Server angegeben.

Führen Sie die folgenden Schritte aus, um das Fehlschlagen des Client-Upgrades zu beheben:

1. Ändern Sie das Verzeichnis in die Position der Protokolldateien.
   - AIX Die Standardposition ist `/usr/tivoli/client/IBM_ANR_UNX/Vxxxx/log`.
   - Linux Die Standardposition ist `/opt/tivoli/tsm/client/IBM_ANR_UNX/Vxxxx/log`.
   - Mac OS X Die Standardposition ist `/Library/Application Support/tivoli/tsm/client/ba/bin/IBM_ANR_MAC/Vxxxx/log`.
   - Windows Die Standardposition ist `C:\Programme\Tivoli\TSM\IBM_ANR_WIN\Vxxxx\log`.

   Hierbei steht das Verzeichnis *Vxxxx* im Pfad für die Zielversion des implementierten Clients für Sichern/Archivieren.
2. Prüfen Sie die Protokoll- und Tracedateien für den Deployment Manager, um die eigentliche Ursache für das Fehlschlagen des Client-Upgrades zu ermitteln. Tabelle 5 zeigt eine Liste der Protokolldateien, die Sie überprüfen können.

Tabelle 5. Beschreibung von Protokolldateien

Protokollname	Beschreibung
`setup.log`	Ein Fehlerprotokoll mit Fehlernachrichten, Warnungen und Informationsnachrichten.
`trace.txt`	Ein Client-Trace mit ausführlichen Informationen zum Client-Upgradeprozess.
`updatemgr.log`	Ein Deployment Manager-Protokoll mit Informationen zum Implementierungsprozess.

Serverstopp beheben

Ein Serverstopp kann aufgrund von Verarbeitungsfehlern, des Trap-Handlers des Systems oder anderen Fehlern auftreten. Wenn Sie die Fehlerquelle für den Serverstopp bestimmen, kann die Ursache auch andere bekannte Probleme beheben.

Der Server kann aus einem der folgenden Gründe stoppen:

- Ein Verarbeitungsfehler hat zur Folge, dass Speicher überschrieben wird, oder ein anderes Ereignis löst die Beendigung des Serverprozesses durch den Trap-Handler des Systems aus.
- Die Serververarbeitung verfügt über Prüfalgorithmen in der gesamten Anwendung, mit denen verschiedene Bedingungen überprüft werden, bevor die Ausführung fortgesetzt wird. Im Rahmen dieser Gültigkeitsprüfung gibt es Fälle, in denen der Server bei fehlgeschlagener Gültigkeitsprüfung selbst die Verarbeitung beendet, anstatt die Fortsetzung der Verarbeitung zu erlauben. Diese fehlgeschlagenen Gültigkeitsprüfungen werden als Konsistenzfehler bezeichnet. Wenn der Server aufgrund eines Konsistenzfehlers beendet wird, wird die folgende Nachricht ausgegeben:

  ```
  ANR7837S Interner
  Fehler XXXNNN wurde erkannt.
  ```

  Dabei ist *XXXNNN* eine Kennung, die dem Konsistenzfehler zugeordnet wird.

Andere Servernachrichten, die auf einen Stopp hinweisen, sind ANR7836S und ANR7838S.

Unabhängig davon, ob der Server aufgrund eines Konsistenzfehlers oder durch den Trap-Handler des Systems gestoppt wurde, kann das Dienstprogramm 'tsmdiag' die folgenden Informationen sammeln und für die Übergabe an den IBM Service paketieren, damit die Situation diagnostiziert werden kann:

- Serverfehlerdatei (`dsmserv.err`)
- Systemimage (Kerndatei)
- Bibliotheken und andere Dateien
- Systemprotokolle
- Aktivitätenprotokoll

Packen Sie alle gesammelten Daten (Dateien) und wenden Sie sich an den IBM Service, um dieses Problem zu melden.

Zugehörige Tasks:

Anhang B, „Dienstprogramm 'tsmdiag' ausführen", auf Seite 213

Stopp oder Schleife beheben

Ein Stopp ist eine Situation, in der der Server keine Funktion startet oder beendet und keinen Mikroprozessorstrom verwendet.

Ein Stopp kann sich nur auf eine Sitzung oder einen Prozess beziehen, die bzw. der nicht verarbeitet wird, oder kann sich auf den gesamten IBM Spectrum Protect-Server beziehen, der nicht antwortet. Eine Schleife ist eine Situation, in der kein Fortschritt erzielt wird, aber der Server in beträchtlichem Maße Mikroprozessorstrom verbraucht. Eine Schleife kann nur eine Sitzung oder einen Prozess oder den gesamten Server betreffen.

Abhängig davon, ob der Server auf Befehle antworten kann, können Sie zur Behebung dieses Fehlertyps Dokumentation sammeln. Es steht ein Perl-Script für das Sammeln von Serverdaten zur Verfügung. Es ist nützlich, die **SHOW**-Befehle regelmäßig auszuführen, sodass Sie das Verhalten bestimmen können, dass der Stoppsituation vorausgeht.

- Wenn der Server auf Befehle antworten kann, geben Sie für einen Stopp oder eine Schleife die folgenden Befehle aus, um die Fehlerursache zu bestimmen:
  - **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** (Geben Sie diesen Befehl nur dann aus, wenn das Problem mit der Zeitplanung zusammenhängt.)

- Wenn ein Server blockiert oder in einer Schleife läuft, geben Sie die folgenden Befehle aus, um eine detaillierte diagnostische Momentaufnahme der IBM Spectrum Protect-Umgebung bereitzustellen:

  ```
  db2fodc -hang -alldbs
  db2support . -d Datenbank -s
  ```

  Sie können die generierte Datei `db2support.zip` für die Fehlerbehebung verwenden.
- Erstellen Sie zusätzlich zur Ausgabe von den aufgelisteten Befehlen oder in Fällen, bei denen ein Server nicht auf Befehle antworten kann, einen Speicherauszug. Die Vorgehensweise bei der Erstellung eines Speicherauszugs hängt vom Betriebssystem ab.
  - AIX Linux Geben Sie den Befehl **KILL -11** im Prozess 'dsmserv' aus, um eine Kerndatei zu erstellen. Um den Befehl „kill" ausführen zu können, rufen Sie die Prozess-ID mit dem Befehl **PS** ab.
  - Windows Suchen Sie auf der Microsoft-Website unter http://support.microsoft.com/ nach Informationen zur Erfassung von Benutzermodusspeicherauszügen.

Wartestatusprobleme bei externen Benutzer-Repository-Servern beheben

Falls der IBM Spectrum Protect-Server nicht zu antworten scheint, kann dieser Umstand auf das Betriebssystem und die Verwendung eines externen Benutzer-Repositorys durch das Betriebssystem zurückzuführen sein.

Vorbereitende Schritte

Ein langsames Leistungsverhalten des Servers kann damit zusammenhängen, dass das Betriebssystem ein externes Benutzer-Repository verwendet, in dem zu viele Benutzergruppen definiert sind. NIS-Server (Network Information Service) und LDAP-Server (Lightweight Directory Access Protocol) sind zwei Typen von externen Benutzer-Repository-Servern.

Ein Beispiel für ein antwortloses Verhalten liegt vor, wenn IBM Spectrum Protect lange benötigt, um eine Verbindung zum IBM DB2-Server herzustellen. Ein weiteres Beispiel ist dann gegeben, wenn der Server scheinbar nicht auf Verwaltungsanforderungen reagiert.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um ein Wartestatusproblem zu beheben, das bei Verwendung eines LDAP-Servers bei den folgenden Servern auftritt:

Vorgehensweise

1. Stoppen Sie den IBM Spectrum Protect-Server.
2. AIX Geben Sie die folgenden Befehle aus:
   a. `db2set DB2_ALTERNATE_GROUP_LOOKUP=GETGRSET`
   b. `db2stop force`
   c. `db2start`

   Linux Geben Sie die folgenden Befehle aus:
   a. `db2set DB2_ALTERNATE_GROUP_LOOKUP=GETGROUPLIST`

b. `db2stop force`

c. `db2start`

3. Starten Sie den Server erneut.

Serverfehlerdatei (`dsmserv.err`) suchen

Wenn der Server stoppt, fügt er der Datei `dsmserv.err`, die sich in demselben Verzeichnis wie der Server befindet, Informationen hinzu.

Vorbereitende Schritte

AIX Linux Der Trap-Handler wird inaktiviert, um zu verhindern, dass das Funktionstraceback Daten an die Konsole und in die Datei `dsmserv.err` ausgibt. Diese Änderung ist erforderlich, um sicherzustellen, dass die Kerndatei vollständig ist. Die Inaktivierung des Trap-Handlers umfasst ein neues Script, `getcoreinfo`, in den Linux-Paketen. Mit dem Script `getcoreinfo` wird das Funktionstraceback für die fehlerhaften Thread- und Registerwerte und das Funktionstraceback für alle anderen Threads abgerufen. Die Informationen, die im Kern für andere Threads verfügbar sind, sind auf einigen Linux-Plattformen bzw. in einigen Linux-Verteilungen immer noch nicht vollständig. Das Script `getcoreinfo` (im Serververzeichnis 'bin') enthält weitere ausführliche Informationen.

Windows Wenn der Server als Dienst ausgeführt wird, hat die Datei den Namen `dsmsvc.err`.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Serverfehlerdatei zu erfassen:

Vorgehensweise

1. Stellen Sie sicher, dass der GNU Debugger (gdb) auf dem Kundensystem installiert ist.
2. Kopieren Sie das Shell-Script gt in das Serververzeichnis 'bin' (in dem sich die ausführbare Datei des Servers [.exe] und die Kerndatei befinden).
3. Stellen Sie sicher, dass es sich bei dem Script um eine ausführbare Datei handelt (`chmod a+x gt`).
4. Rufen Sie das Script mit den Pfaden/Namen der ausführbaren Datei (der Standardwert ist `./dsmserv`) und der Kerndatei (der Standardwert ist `./dsmcore`) auf. Die Ausgabe wird in die Datei `dsm_gdb.info` gestellt (die an IBM gesendet werden sollte).

Systemimage (Kerndatei) suchen

Normalerweise wird eine Kerndatei oder ein anderes Systemimage des Speichers von IBM Spectrum Protect verwendet, wenn der Fehler auftritt.

Benennen Sie die Kerndatei in jedem Fall um, damit sie bei einem späteren Stopp nicht überschrieben wird. Beispielsweise sollte eine Datei in „core.Aug29" und nicht nur in „core" umbenannt werden. Der Typ und Name der Kerndatei variieren abhängig von der Plattform:

- AIX Linux Normalerweise wird eine Datei namens `core` erstellt. Stellen Sie sicher, dass im Serververzeichnis genügend Speicherbereich für eine Speicherauszugsoperation vorhanden ist. Normalerweise hat eine Speicherauszugsdatei für den IBM Spectrum Protect-Server (32-Bit) 2 GB. Stellen Sie außerdem

sicher, dass 'ulimit' für Kerndateien auf 'unbegrenzt' gesetzt ist, damit die Speicherauszugsdatei nicht abgeschnitten wird.

- Windows Vom Inhalt des Systems wird automatisch ein Speicherauszug über einen API-Systemaufruf erstellt. Wird der Server als Dienst ausgeführt, lautet die Speicherauszugsdatei `dsmsvc.dmp`. Andernfalls lautet die Speicherauszugsdatei `dsmserv.dmp`.

Wenn das System nicht für die Erfassung einer Kerndatei konfiguriert wurde oder das System nicht genügend Speicherbereich für die Erstellung einer vollständigen Kerndatei hatte, ist die Datei möglicherweise für die Fehlerbestimmung nur begrenzt verwendbar.

Bibliotheksdateien für Kernanalyse abrufen

AIX Linux

Kerndateien gelten speziell für die Anwendung, die Bibliotheken und andere Systemressourcen, die von der Anwendung auf dem System verwendet werden, auf dem sie ausgeführt wird.

Um die Kerndatei auf Ihrem Computersystem genau zu lesen, benötigen Sie alle folgenden Dateien, die sich in dem Verzeichnis befinden, in dem der Server installiert ist:

- `dsmserv`
- `dsmlicense`
- `ndmpspi`
- `dsmcored`
- `dsmaio`
- `centera`

Die Bibliotheksdateien, die benötigt werden, variieren zwischen allen Plattformen:

- AIX Sammeln Sie die folgenden Dateien:
  - `/usr/ccs/lib/libpthreads.a`
  - `/usr/ccs/lib/libc.a`
  - Sammeln Sie alle anderen geladenen Bibliotheken, wie z. B. Nachrichtenexits. Um zu bestimmen, welche Bibliotheken geladen sind, rufen Sie 'dbx' auf, indem Sie den Befehl **`dbx dsmserv core_file`** ausgeben. Geben Sie dann in der dbx-Eingabeaufforderung den Befehl **`map`** aus, um alle Bibliotheken anzuzeigen, die geladen sind und für die Kernanalyse benötigt werden.
- Linux Geben Sie den Befehl **`ldd dsmserv`** aus und sammeln Sie alle dynamischen gemeinsam genutzten Bibliotheken. Beispiel:
  - `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`

Systemprotokolldateien abrufen

Sie können Systemprotokolldateien abrufen, um die Ursachen für Serverstopps zu beheben.

Rufen Sie die folgenden Protokolldateien für den IBM Service ab:

- AIX Leiten Sie die Ausgabe des Befehls **errpt -a** in eine Datei um: `errpt -a >errpt.txt`.
- Linux Kopieren Sie die Datei `/var/log/messages`.
- Windows Speichern Sie eine Kopie der Ereignisprotokolle (wie in der Ereignisanzeige angezeigt).

Aktivitätenprotokoll abrufen

Aktivitätenprotokolldateien können abgerufen werden, um Probleme mit einem Serverstopp zu beheben.

Fragen Sie die Einträge im Aktivitätenprotokoll ab, die mindestens zwei Stunden vor dem Stopp und 30 Minuten nach dem Stopp aufgezeichnet wurden, indem Sie den Befehl **QUERY ACTLOG** ausgeben.

Fehler nach dem Starten und Stoppen eines Serverservice erkennen

Windows

Wenn ein Serverservice unerwartet gestartet und gestoppt wird, können Sie die Fehlerursache bestimmen, indem Sie eine Fehlerprotokolldatei anfordern.

Informationen zu diesem Vorgang

Ein Service (Dienst) kann über das Applet für Windows-Dienste gestartet werden. Nachdem Sie den Service gestartet haben, zeigt der Service möglicherweise an, dass er gestartet wurde, nach der Aktualisierung zeigt er jedoch an, dass er gestoppt wurde. In den folgenden Schritten wird „Server1" als der Name des Servers verwendet, der gestartet und gestoppt wird. Um die Ursache des Fehlers für Server1 zu bestimmen, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Erweitern Sie **Tivoli Storage Manager** > **[*Hostname*] (Windows - Lokal)** > **Server1** > **Berichte** > **Serviceinformationen**, um den Serverservice anzuzeigen.
2. Klicken Sie im rechten Teilfenster mit der rechten Maustaste auf den Service **Server1** und wählen Sie **Merkmale** aus.
3. Wählen Sie die Option **Ausgabe in Datei protokollieren** aus und klicken Sie auf **OK**.
4. Starten Sie den Service Server1.
5. Wenn der Service erneut gestoppt wird, öffnen Sie einen Texteditor, um den Inhalt der folgenden Datei zu lesen:

   `C:\Programme\Tivoli\TSM\Server1\console.log`
6. Bestimmen Sie die Fehlerursache, indem Sie die generierten Fehlernachrichten überprüfen.

Verzeichnis sqllib/db2dump verursacht Beendigung

Tivoli Storage Manager-Server der Version 6 können unerwartet beendet werden, wenn das Verzeichnis `sqllib/db2dump` zu voll wird. Eine Beendigung tritt am häufigsten zu dem Zeitpunkt auf, zu dem DB2 FODC-Dateien (FODC = First Occurrence Data Capture) in das Verzeichnis geschrieben werden.

Das Verzeichnis `sqllib/db2dump` ist ein Diagnosedatenverzeichnispfad, den DB2 zum Schreiben von Diagnoseinformationen für FODC verwendet. Im Laufe der Zeit kann DB2 viele FODC-Dateien in das Verzeichnis schreiben, die sich auf den fehlerfreien Zustand der Datenbank beziehen. Wenn Dateien nicht entfernt oder gelöscht werden, kann sich das Dateisystem füllen. Die Position der DB2 FODC-Dateien hängt von Ihren DB2-Konfigurationseinstellungen oder den Einstellungen der DB2-Umgebungsvariablen ab.

Lokalisieren Sie das Diagnosedatenverzeichnis, indem Sie die DB2-Konfigurationseinstellungen oder die Einstellungen der DB2-Umgebungsvariablen überprüfen. Wenn die Dateien im Diagnoseverzeichnispfad zur Folge haben, dass das Dateisystem voll wird, führen Sie eine der folgenden Aktionen aus:

- Fügen Sie dem Dateisystem Speicherbereich hinzu.
- Versetzen Sie die Dateien in ein anderes Dateisystem. Siehe Tabelle 6.
- Verwenden Sie den Server, um die Dateien zu archivieren. Löschen Sie anschließend die Dateien, indem Sie die folgenden Schritte ausführen:
  1. Führen Sie das Dienstprogramm 'db2support' aus, um die DB2-Systemdiagnoseinformationen zu erfassen.
  2. Archivieren Sie mit dem Client die Datei `db2support.zip` und die Diagnosedateien, die in Tabelle 6 aufgelistet sind, auf dem Server.
  3. Löschen Sie die Dateien, die in Tabelle 6 aufgelistet sind.

Tabelle 6. Dateien, die nach ihrer Archivierung gelöscht werden können

Dateiname	Beschreibung
`instance_name.nfy` `instance_name.`*`n`*`.nfy` (dabei ist *n* eine Zahl)	Protokolle mit Benachrichtigungen für die Systemverwaltung
`db2dasdiag.log`	Diagnoseprotokoll für DB2-Verwaltungsserver
`db2eventlog.`*`xxx`* (dabei ist *xxx* die Nummer der Datenbankpartition)	DB2-Ereignisprotokoll
`nnnnnnn.nnnnn.nnn``.dump.bin` (dabei ist *n* eine Zahl)	Binäre Speicherauszugsdateien von wichtigen speicherinternen Strukturen
`nnnnnnn.n.nnn``.trap.txt` (dabei ist *n* eine Zahl)	Trapdateien
`nnnnnnn.nnnnn.nnn``.apm.bin` (dabei ist *n* eine Zahl)	Binäre Speicherauszugsdateien für Planmanager
`nnnnnnn.nnnnn.nnn``.stack.txt` (dabei ist *n* eine Zahl)	Stack-Traces

Tabelle 6. Dateien, die nach ihrer Archivierung gelöscht werden können (Forts.)

Dateiname	Beschreibung
FODC_*xxxx*/core<pid>	Kerndateien Diese Verzeichnisse FODC_*xxx* enthalten die Zeitmarke im Verzeichnisnamen. Bewahren Sie die neuesten Verzeichnisse und deren Dateien auf. Das Protokoll kann bei der Diagnose möglicher zukünftiger Probleme, die im Zusammenhang mit der Datenbank auftreten, hilfreich sein. Als Richtlinie sollten Sie mindestens die Verzeichnisse und Dateien einer Woche aufbewahren.
events/db2optstats.*n*.log (dabei ist *n* eine Zahl)	Statistikprotokolldatei

Tipp: Löschen Sie nicht die Datei db2diag.log und die Dateien im Verzeichnis stmmlog. Das darin enthaltene Protokoll kann bei der Diagnose von Serverproblemen, die im Zusammenhang mit der Datenbank auftreten, nützlich sein.

Zugehörige Verweise:

„DB2-Diagnoseprotokolldateien lokalisieren" auf Seite 79

Probleme bei der Datenbankseitenprüfung beheben

Ein Seitenauswertungsfehler während der Datenbanksicherungsverarbeitung kann auf eine Beschädigung der Datenbank hinweisen und erfordert eine Reparaturaktion zur Behebung des Problems. Wenn die Seitenauswertung fehlschlägt, schlägt auch die Datenbanksicherung fehl.

Vorgehensweise

- Bitten Sie den IBM Support um Unterstützung bei der Diagnose und Reparatur einer Datenbankbeschädigung.
- Wenn gerade eine Datenbankgesamtsicherung aktiv war, um Speicherplatz im Archivprotokollverzeichnis freizugeben, führen Sie eine der folgenden Aktionen aus:
  - Stellen Sie mehr Speicherplatz im Archivprotokollverzeichnis bereit.
  - Geben Sie die Option ARCHFAILOVERLOGDIRECTORY an, um ein Archivübernahmeprotokollverzeichnis anzugeben, in dem der Server Protokolldateien speichern kann, die nicht im Archivprotokollverzeichnis gespeichert werden können.

  Wenn genügend Speicherplatz im Archivprotokollverzeichnis zur Verfügung steht, kann der Server weiter ausgeführt werden, während die Datenbank repariert wird.

Datenbankfehler beheben

Datenbankfehler können durch Probleme wie Speicherplatzengpässe und durch Fehler verursacht werden, die auf Einfüge-, Aktualisierungs- oder Löschoperationen zurückzuführen sind.

Benutzer, die erfahrene DB2-Administratoren sind, können erweiterte SQL-Abfragen ausführen und DB2-Tools verwenden, um die Datenbank, den verwendeten Speicherplatz und gegebenenfalls auftretende Fehler zu überwachen. Verwenden Sie jedoch bei einer Ausführung dieser Abfragen keine DB2-Tools, um DB2-Konfigurationseinstellungen zu ändern, die von IBM Spectrum Protect voreingestellt sind. Ändern Sie diese Einstellungen auch nicht mit einer anderen Software. Der Server muss mit der Datendefinitionssprache und der Datenbankkonfiguration verwendet werden, die IBM Spectrum Protect implementiert.

Weitere Informationen finden Sie in der Produktinformation zu DB2.

Probleme beim Starten des Datenbankmanagers beheben

Der IBM Spectrum Protect-Server wird möglicherweise nicht gestartet, wenn der DB2-Datenbankmanager für die Verwendung des Plug-ins `dsmdb2pw` konfiguriert ist. Wenn der Server das Plug-in nicht laden kann, wird der Datenbankmanager nicht gestartet und kann umgekehrt der Server nicht gestartet werden.

Aufgrund des Plug-in-Problems gibt der Server eine ähnliche Fehlernachricht wie im folgenden Beispiel aus:

```
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 = "".
```

Möglicherweise erhalten Sie auch diese Fehlernachricht:

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

Überprüfen Sie die Datei `db2diag.log` auf Diagnoseinformationen bezüglich dieses Fehlertyps.

Beispiel aus der Datei `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/sqllib/security64/plugin/server/dsmdb2pw.so
CALLSTCK:
  [0] 0x00002AEF63DD267E pdOSSeLoggingCallback + 0x20C
  [1] 0x00002AEF68486A42 /home/hannigan/sqllib/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 _Z25sqlexLoadAllPluginsServerP5sqlca + 0x3B5
  [7] 0x00002AEF6431737C /home/hannigan/sqllib/lib64/libdb2e.so.1 + 0x123637C
  [8] 0x00002AEF643164C5 sqloRunInstance + 0x191
```

```
  [9] 0x000000000040D31D 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/sqllib/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 _Z25sqlexLoadAllPluginsServerP5sqlca + 0x3B5
  [7] 0x00002AEF6431737C /home/hannigan/sqllib/lib64/libdb2e.so.1 + 0x123637C
  [8] 0x00002AEF643164C5 sqloRunInstance + 0x191
  [9] 0x000000000040D31D DB2main + 0xD41
```

Beim Start erkennt der Server diese Fehlertypen und der Server versucht, das Plug-in aus der Konfiguration zu entfernen. Wenn der Server das Plug-in nicht entfernen kann, müssen Sie das Plug-in aus der Konfiguration des Datenbankmanagers entfernen. Mit dem folgenden Befehl wird das Plug-in aus der Konfiguration des Datenbankmanagers entfernt:

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

Traceerstellung für das Plug-in für Benutzer-ID und Kennwort

Falls korrekt konfiguriert, kann der Server automatisch einen Trace für das Plug-in für die Benutzer-ID und das Kennwort (`dsmdb2pw`) durchführen.

Um die automatische Traceerstellung für das Plug-in für Benutzer-ID und Kennwort zu definieren, führen Sie die folgenden Schritte aus:

AIX Linux

1. Stellen Sie sicher, dass der Server über Schreibberechtigung für das Verzeichnis `~/sqllib/db2dump/` verfügt.
2. Fügen Sie den folgenden Text zur Datei `~instance/sqllib/userprofile` hinzu:
   ```
   export DB2_DSMDB2PW_TRACEFILE=Dateiname
   ```
   Hierbei steht *Dateiname* für den vollständig qualifizierten Pfad und den Namen der Tracedatei, z. B. `~/sqllib/db2dump/dsmdb2pw.trc`.
3. Starten Sie DB2 erneut.

Nach dem Neustart von DB2 wird die Traceausgabe in der angegebenen Datei und dem angegebenen Verzeichnis gespeichert.

Windows

1. Um zu prüfen, ob `DB2_VENDOR_INI db2set` definiert ist, führen Sie den Befehl `db2set` aus.
2. Ist die Variable *DB2_VENDOR_INI* nicht definiert, erstellen Sie eine Konfigurationsdatei. Beispiel:

```
c:\Programme\Tivoli\TSM\s1\tsmdbmgr.env
```

3. Aktualisieren Sie die Konfigurationsdatei, die in *DB2_VENDOR_INI* aufgelistet ist, mit der Position der Tracedatei:
   ```
   DB2_DSMDB2PW_TRACEFILE=c:\Programme\Tivoli\TSM\s1\sqllib\dsmdb2pw.trc
   ```
4. Definieren Sie die Tracedatei, indem Sie den folgenden Befehl ausgeben:
   ```
   db2set -i Serverinstanz DB2_VENDOR_INI=Position_der_Konfigurationsdatei
   ```

   Beispiel:
   ```
   db2set -i s1 DB2_VENDOR_INI=c:\Programme\Tivoli\TSM\s1\tsmdbmgr.env
   ```
5. Stoppen Sie den IBM Spectrum Protect-Server und starten Sie ihn erneut, indem Sie die folgenden Befehle ausgeben:
   ```
   halt
   dsmserv -k Serverinstanz
   ```

Nach dem Serverneustart wird die Traceausgabe in der angegebenen Datei und dem angegebenen Verzeichnis gespeichert.

Tipp: Sie können einen Dateinamen und ein Verzeichnis Ihrer Wahl für den Namen und die Position der Tracedatei verwenden.

DB2-Speicherzuordnung begrenzen

Wenn DB2 eine große Speichermenge nutzt, können Sie die Speichermenge begrenzen, die von DB2 verwendet wird, indem Sie den Befehl **db2 update** ausgeben.

Informationen zu diesem Vorgang

Standardmäßig wird DB2 mit automatischer Speicherverwaltung installiert und konfiguriert. Dies hat zur Folge, dass DB2 einen hohen Prozentsatz des physischen Speichers verwendet. Zur Begrenzung der Speichermenge geben Sie mit dem Befehl **db2 update** den Grenzwert für den Speicher an.

Vorgehensweise

Geben Sie den Befehl **db2 update** aus:

```
db2 update dbm cfg using instance_memory Speicherwert
```

Hierbei wird *Speicherwert* in Blöcken von 4 KB angegeben.

Beispiel

Um die Speicherzuordnung für DB2 auf 3.200.000 KB zu begrenzen, müssen Sie 3.200.000 KB durch 4 KB dividieren. Das Ergebnis ist 800.000. Geben Sie anschließend den folgenden Befehl aus:

```
db2 update dbm cfg using instance_memory 800000
```

Weitere Informationen zur Instanzspeicherkonfiguration finden Sie in der Produktinformation zu DB2.

DB2-Versionsinformationen abrufen

Die Version von DB2, die mit dem IBM Spectrum Protect-Server installiert wird, wird regelmäßig aktualisiert. Falls Datenbankfehler auftreten, müssen Sie die Version und die Position von DB2 kennen, um diese Informationen dem IBM Software Support mitteilen zu können.

Vorgehensweise

Geben Sie den Befehl **db2level** aus, um die Installationsposition der DB2-Produkte auf Ihrem Server anzuzeigen und die DB2-Produktversion aufzulisten.
Ein Beispiel für die Ausgabe des Befehls **db2level** ist nachfolgend dargestellt.

AIX Linux

```
> db2level
DB21085I Diese Instanz oder Installation (Instanzname, sofern zutreffend:
"cetinst1") verwendet "64" Bit und DB2-Codefreigabe "SQL10051" mit
Aktualitäts-ID "0602010E".
Informationstoken sind "DB2 v10.5.0.1", "special_31150",
"IP23526_31150" und Fix Pack "1".
Produkt ist installiert unter "/opt/tivoli/tsm/db2".
```

Windows

```
C:\>db2level
DB21085I  Diese Instanz oder Installation (Instanzname, sofern zutreffend: "SERVER")
verwendet "64 Bit" und DB2-Codefreigabe "SQL10051" mit Aktualitäts-ID
"0602010E".
Informationstoken sind "DB2 v10.5.100.64", "special_31150",
 "IP23521_31155" und Fix Pack "1".
Product is installed at "C:\PROGRA~1\Tivoli\TSM\db2" with DB2 Copy Name "DB2TSM1".
```

DB2-Diagnoseprotokolldateien lokalisieren

Die Datei `db2diag.log` enthält Diagnoseinformationen, die Ihnen helfen können, Probleme mit Ihrer Datenbank zu beheben.

Die Position der Datei `db2diag.log` und der DB2 FODC-Dateien hängt von Ihren DB2-Konfigurationseinstellungen oder den Einstellungen der DB2-Umgebungsvariablen ab. DB2 schreibt Nachrichten zu internen Operationen, zu Ereignissen oder zum Status in die Protokolldatei mit Benachrichtigungen für die Systemverwaltung (`db2SID.nfy`).

AIX Linux Führen Sie die folgenden Schritte aus, um zu bestimmen, wo sich der Pfad für das Diagnosedatenverzeichnis befindet:

1. Melden Sie sich als Serverbenutzerinstanz an.
2. Geben Sie den folgenden Befehl aus:

   ```
   db2 get dbm cfg | grep DIAGPATH
   ```

   Wenn im Konfigurationsparameter **DIAGPATH** kein Pfad angegeben ist, befindet sich das Diagnosedatenverzeichnis im Unterverzeichnis `sqllib/db2dump` des Instanzverzeichnisses. Beispiel: `/home/tsminst1/sqllib/db2dump`, wobei `/home/tsminst1` das Instanzausgangsverzeichnis ist.

Windows Führen Sie die folgenden Schritte aus, um zu bestimmen, wo sich der Pfad für das Diagnosedatenverzeichnis befindet:

1. Stoppen Sie den interaktiven DB2-Modus. Starten Sie eine DB2-Eingabeaufforderung und geben Sie den Befehl `quit` aus.

2. Suchen Sie den Pfad, indem Sie den Konfigurationsparameter **DIAGPATH** verwenden. Geben Sie den folgenden Befehl aus:

   ```
   db2 get dbm cfg | findstr /s /i diagpath
   ```

3. Wenn im Konfigurationsparameter **DIAGPATH** kein Pfad angegeben ist, wird der Verzeichnispfad DB2INSTPROF verwendet. Suchen Sie den Pfad, der in der Umgebungsvariablen *DB2INSTPROF* definiert wurde. Geben Sie den folgenden Befehl in der DB2-Eingabeaufforderung aus:

   ```
   db2set db2instprof
   ```

   Die Ausgabe dieses Befehls zeigt die Position von DB2-Datendateien. Die Diagnoseprotokolldatei befindet sich im Instanzunterverzeichnis des Verzeichnisses, das durch die Registry-Variable *DB2INSTPROF* angegeben ist. Für die Serverinstanz TSMSERVER1 zeigt der Befehl **db2set deb2instprof** beispielsweise den folgenden Pfad an:

   ```
   C:\ProgramData\IBM\DB2\DB2TSM1
   ```

   Die Diagnoseprotokolldatei befindet sich im Unterverzeichnis TSMSERVER1:

   ```
   C:\ProgramData\IBM\DB2\DB2TSM1\TSMSERVER1
   ```

4. Falls die Umgebungsvariable *DB2INSTPROF* nicht definiert ist, wird der Pfad x:\SQLLIB\DB2INSTANCE verwendet. x:\SQLLIB ist der Laufwerksverweis und ebenfalls das Verzeichnis, das in der Registry-Variablen *DB2PATH* angegeben ist. Der Wert von *DB2INSTANCE* ist der Name der Instanz. Das Verzeichnis SQLLIB muss nicht aufgerufen werden. Der erste Teil der Ausgabe für den Befehl **db2set db2path** ist der Pfad des Diagnosedatenverzeichnisses mit dem hinzugefügten Instanznamen. Die Ausgabe zeigt den folgenden Verzeichnispfad:

   ```
   C:\Programme\Tivoli\TSM\db2\TSMINST1
   ```

   Hierbei steht *DB2PATH* für C:\Programme\Tivoli\TSM\db2 und der Instanzname lautet TSMINST1.

Zugehörige Verweise:

„Installationsprotokolldateien” auf Seite 64

DB2-Upgradeprotokolldateien

Bei einem Upgrade des IBM Spectrum Protect-Servers wird das DB2-Script **db2ckupgrade** ausgeführt. Dieses Script erstellt Protokolldateien für die Serverdatenbanken.

Während des Upgrades korrigiert der Assistent manche Fehler in der Datenbank automatisch. Andere Fehler müssen Sie manuell beheben. Anhand der Protokolldateien können Sie feststellen, welche Fehler Sie beheben müssen. Die Protokolldateien enthalten die Ergebnisse, die vom Befehl **db2ckupgrade** für jede Datenbank erzielt wurden.

Die folgenden Protokolldateien werden bei der Durchführung eines Upgrades erstellt:

- AIX Linux /tmp/db2ckupgrade_*Instanzname_DB-Name*.log
- Windows *Installationsverzeichnis*\db2ckupgrade_*Instanzname_DB-Name*.log

Falls Sie bei der Ausführung des Scripts eine Nachricht über einen Datenbankfehler empfangen, der vom Assistenten nicht behoben wird, müssen Sie den Assistenten abbrechen oder schließen, den Fehler korrigieren und das Upgrade erneut starten. Bei einer unbeaufsichtigten Installation müssen Sie überprüfen, ob in der Datei log.text Fehler angegeben sind. Korrigieren Sie alle in dieser Datei angegebenen

Fehler und starten Sie das Upgrade erneut. Details zu Fehlernachrichten, die in den Protokolldateien aufgeführt sind, finden Sie in der Produktinformation zu DB2.

Problem mit fehlender oder falscher Datenbank-ID-Datei beheben

Wenn Sie eine Datenbank nach einem Katastrophenfall auf einen anderen Server zurückschreiben, wird die Datenbank-ID-Datei (`dsmserv.dbid`) möglicherweise nicht zurückgeschrieben. Der IBM Spectrum Protect-Server kann daher die Datei nach der Zurückschreibungsoperation nicht finden und kann nicht gestartet werden.

Nach der Durchführung eines Upgrades von Tivoli Storage Manager Version 6.1 auf 6.2 können bei der Zurückschreibung von Tivoli Storage Manager Version 6.1-Datenbanken Schwierigkeiten auftreten. Sie müssen den Tivoli Storage Manager-Server der Version 6.2 starten, um ein neues Sicherungsimage in DB2 zu generieren. Nach der Initialisierung des Tivoli Storage Manager-Servers der Version 6.2 wird automatisch eine Datenbanksicherung gestartet. Wenn die Sicherung abgeschlossen ist, stoppen Sie den Server und geben Sie den Befehl **RESTORE DB** aus. Wird die automatische Datenbanksicherung nicht erfolgreich ausgeführt, beheben Sie das Problem und geben Sie den Befehl **BACKUP DB** aus. Stellen Sie sicher, dass die Sicherung ausgeführt wird, bevor Sie den Befehl **RESTORE DB** ausgeben.

Wichtig: Ein Datenbanksicherungsimage muss vom Tivoli Storage Manager-Server der Version 6.2 erfolgreich generiert worden sein, damit Teilsicherungen der Datenbank oder Datenbankzurückschreibungen erfolgreich ausgeführt werden können.

Wenn Sie den Tivoli Storage Manager-Server der Version 6.2, für den ein Upgrade durchgeführt wurde, gestartet haben und die automatische Datenbanksicherung erfolgreich abgeschlossen wurde, können Sie die Datenbank vor der Zurückschreibung löschen. Sie dürfen die Datenbank nicht sofort nach dem Upgrade auf Version 6.2 löschen. Wenn Sie die Datenbank löschen, bevor ein Sicherungsimage generiert wurde, müssen Sie den Tivoli Storage Manager-Server der Version 6.1 erneut installieren und dann die Datenbank zurückschreiben.

Wenn Sie eine Tivoli Storage Manager Version 6.1-Datenbank zurückschreiben müssen und die Datenbank nicht vorhanden ist, müssen Sie die Datenbank über Tivoli Storage Manager Version 6.1 wiederherstellen. Anschließend können Sie ein Upgrade auf Tivoli Storage Manager Version 6.2 durchführen.

Eine nicht mehr vorhandene oder falsche Datei `dbid` kann nach einer Datenbankzurückschreibungsoperation Auswirkungen auf das Starten des Servers haben.

Wenn eine Datenbank zurückgeschrieben wird, muss die Datenbank-ID-Datei mit der Datenbank synchron bleiben. Wird die Datenbank mit Tivoli Storage Manager Version 6.2 formatiert, bevor sie zurückgeschrieben wird, ändert sich die Datei mit den Datenbank-IDs. Diese Änderung führt zu einer Abweichung des Datums und der Uhrzeit in der Datenbank und verhindert das Starten des Servers.

Wenn Ihre Datenbank-ID-Datei während einer Zurückschreibungsoperation Fehler verursacht, müssen Sie möglicherweise den Parameter -S (DB-ID-Überprüfung überspringen) verwenden. Die Datei `dsmserv.dbid` darf auf Ihrem Server nicht vorhanden sein, wenn Sie den Parameter -S verwenden. Nachfolgend werden Situationen beschrieben, in denen der Parameter -S nützlich ist:

- Wird der Server nach der Sicherung neu formatiert, ist eine Abweichung des Datums und der Uhrzeit in der neuen Datei `dsmserv.dbid` die Folge. Verwenden Sie den Parameter -S, wenn der Server nach der Zurückschreibung gestartet wird.
- Wenn die Datei `dsmserv.dbid` beschädigt ist oder verloren geht.

Nach der ersten Verwendung des Parameters -S in einem Zurückschreibungsszenario erstellt der Server eine Datei `dsmserv.dbid` im Instanzverzeichnis.

Fehler für die Befehle BACKUP DB und RESTORE DB beheben

Die Serverbefehle **BACKUP DB** und **RESTORE DB** fordern die IBM DB2-Datenbankanwendung auf, die IBM Spectrum Protect-Datenbank auf dem Server zu sichern.

Sicherungsdaten werden dann über die Anwendungsprogrammierschnittstelle (API) für den Client an den Server gesendet.

Wenn ein Befehl **BACKUP DB** oder **RESTORE DB** mit einem DB2-SQLCODE oder einer SQLERRMC-Nachricht mit Rückkehrcodes fehlschlägt, rufen Sie eine Beschreibung des DB2-SQLCODE ab, indem Sie die folgenden Prozeduren ausführen:

1. Öffnen Sie eine DB2-Befehlszeilenschnittstelle:

   Windows Klicken Sie für Windows auf **Start** > **Alle Programme** > **IBM DB2** und klicken Sie auf **Befehlszeilentools** > **Befehlszeilenprozessor**.

   AIX Linux Melden Sie sich für alle anderen unterstützten Plattformen bei der DB2-Instanz-ID an und öffnen Sie ein Shellfenster. Geben Sie dann den Befehl `DB2` aus.
2. Geben Sie den SQLCODE ein. Lautet z. B. der DB2-SQLCODE -2033, geben Sie den folgenden Befehl aus:

   ```
   ? sql2033
   ```

Sie können die Details der Fehlerbedingung verwenden, um den Fehler für den Befehl **BACKUP DB** oder **RESTORE DB** zu beheben. Wird auch der SQLERRMC-Code angezeigt, wird er in der bereitgestellten SQLCODE-Beschreibung erläutert. Weitere Informationen zu den API-Rückkehrcodes befinden sich in den folgenden Dateien:

- Windows `tsm\api\include\dsmrc.h`
- AIX Linux `tsm/client/api/bin64/sample/dsmrc.h`

Falsche Umgebungsvariablen für BACKUP DB und RESTORE DB korrigieren

Viele der Verarbeitungsprobleme, die bei **BACKUP DB** oder **RESTORE DB** auftreten, sind auf eine falsch definierte Umgebungsvariable DSMI_CONFIG, DSMI_DIR oder DSMI_LOG zurückzuführen.

Informationen zu diesem Vorgang

Voraussetzung:
Die Umgebungsvariablen werden von der Client-API zum Lokalisieren des API-Codes und der Optionsdateien verwendet. Die DB2-Instanz muss in einer Shell mit korrekt definierten Umgebungsvariablen ausgeführt werden.

AIX Linux Die Variablen DSMI_* werden in der Datei `userprofile` der Instanz definiert. Beispiel: `/home/tsminst1/sqllib/userprofile`

Windows Die Variablen DSMI_* werden in der Datei definiert, auf die die Variable für die DB2-Instanzregistry, DB2_VENDOR_INI, verweist. Diese Datei kann bei-

spielsweise `c:\tsminst1\tsmdbmgr.env` sein. Sie können den Dateinamen und die Position überprüfen, indem Sie den Befehl `db2set -i tsminst1 DB2_VENDOR_INI` ausgeben; dabei ist tsminst1 die DB2-Instanz.

Die Variablen DSMI_* werden anfänglich automatisch vom IBM Spectrum Protect-Assistenten für Instanzkonfiguration konfiguriert.

Vorgehensweise

Öffnen Sie die Datei `/home/tsminst1/sqllib/userprofile` und überprüfen Sie die Anweisungen. Wenn Sie diese Datei ändern, stoppen Sie die DB2-Instanz und starten Sie sie erneut, damit die Änderungen berücksichtigt werden. Betrachten Sie beispielsweise das folgende Szenario. Die Datei `userprofile` enthält ähnliche Anweisungen wie der folgende Beispieltext:

```
export DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
export DSMI_DIR=Verzeichnis_server_bin/dbbkapi
export DSMI_LOG=Serverinstanzverzeichnis
```

Die Datei `tsmdbmgr.opt` enthält den folgenden Text:

```
SERVERNAME TSMDBMGR_TSMINST1
```

Die Datei *Verzeichnis_server_bin*`/dbbkapi/dsm.sys` enthält den folgenden Text:

```
SERVERNAME TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
errorlogname /tsminst1/tsmdbmgr.log
```

Überprüfen Sie, ob der Eintrag SERVERNAME in der Datei `tsmdbmgr.opt` mit dem Eintrag SERVERNAME in der Datei `dsm.sys` übereinstimmt.

Linux Fügen Sie nicht die Option `PASSWORDACCESS GENERATE` zur Konfigurationsdatei `dsm.sys` hinzu. Diese Option kann dazu führen, dass die Datenbanksicherung fehlschlägt.

Fehlernachricht ANR2968E beheben

Die Fehlernachricht ANR2968E kann während der Ausführung des Befehls **BACKUP DB** auftreten.

Informationen zu diesem Vorgang

Es gibt zwei Ursachen für diese Fehlernachricht:

- Der Eigner der IBM Spectrum Protect-Fehlerprotokolldatei ist die Rootbenutzer-ID und nicht die Benutzer-ID der Serverinstanz.
- Windows Die Pfade in der Datei `tsmdbmgr.env` sind in Anführungszeichen eingeschlossen. Verwenden Sie einen Pfad, der keine Leerzeichen enthält, oder verwenden Sie den Windows-Kurznamen für den Pfad.

Ist die Rootbenutzer-ID Ursache des Fehlers, führen Sie die folgenden Schritte aus, um den Fehler zu beheben:

Vorgehensweise

1. Melden Sie sich unter Verwendung einer IBM Spectrum Protect-Serverinstanz-ID an und überprüfen Sie den Namen der Fehlerprotokolldatei. Beispiel:

   ```
   $ grep -i "FEHLERPROTOKOLLNAME" $DSMI_DIR/dsm.sys
   FEHLERPROTOKOLLNAME /home/db2inst1/tsminst1/tsmdbmgr.log
   ```

Dabei ist db2inst1 die Benutzer-ID der Serverinstanz und /home/db2inst1/tsminst1/ das Serverinstanzverzeichnis.

2. Geben Sie den folgenden Beispielbefehl aus, um zu überprüfen, wer der aktuelle Eigner der Fehlerprotokolldatei ist:

```
$ ls -la /home/db2inst1/tsminst1/tsmdbmgr.log
-rw-r--r-- 1 root system 834 May 05 09:43 /home/db2inst1/tsminst1/tsmdbmgr.log
```

3. Ist der Eigner der Fehlerprotokolldatei nicht die IBM Spectrum Protect-Instanzbenutzer-ID, entfernen Sie die Datei. Um die Datei entfernen zu können, müssen Sie über Rootberechtigung verfügen. Geben Sie den folgenden Beispielbefehl aus, um die Protokolldatei zu entfernen:

```
$ su Rootkennwort
# rm /home/db2inst1/tsminst1/tsmdbmgr.log
# exit
```

4. Geben Sie den Befehl **BACKUP DB** aus und überprüfen Sie, ob der Befehl erfolgreich ausgeführt wurde. Überprüfen Sie, ob die Serverinstanz-ID der Eigner der Protokolldatei ist. Beispiel:

```
$ ls -la /home/db2inst1/tsminst1/tsmdbmgr.log
-rw-r--r-- 1 db2inst1 db2iadm1 834 May 05 09:50
/home/db2inst1/tsminst1/tsmdbmgr.log
```

Fehlernachricht ANR2971E mithilfe des SQL-Codes beheben

Fehlernachricht ANR2971E wird möglicherweise angezeigt, wenn Sie eine Datenbank zurückschreiben oder sichern und der Prozess stoppt. Beheben Sie dieses Problem mithilfe des in der Fehlernachricht angegebenen SQL-Codes.

Vorbereitende Schritte

Wenn Sie eine Datenbank zurückschreiben, weil der Server während des normalen Betriebs gestoppt wurde, überprüfen Sie die Datei db2diag.log, *bevor* Sie die Datenbank sichern oder zurückschreiben.

Die folgende Nachricht kann ausgegeben werden, wenn Sie Daten zurückschreiben oder sichern:

```
ANR2971E Sicherung/Zurückschreibung/Rollforward der Datenbank beendet -
Fehler mit DB2-SQLCODE -2581
```

In dem folgenden Szenario ist der Prozess **DSMSERV RESTORE DB** mit dem DB2 SQL-Code 2581 fehlgeschlagen. Das folgende Szenario gilt nicht für Probleme mit den DSMI-Umgebungsvariablen.

Vorgehensweise

1. Geben Sie in der DB2-Befehlszeilenschnittstelle den folgenden Befehl aus:

```
? SQL2581
```

   Es wird eine Erläuterung zu dem SQL-Code generiert.

```
SQL2581N  Der Restore kann keine Protokolldateien aus dem Backup-Image
in den angegebenen Pfad extrahieren bzw. für ein Protokollverzeichnis
kein Restore aus dem Backup-Image in den angegebenen Pfad durchführen.
Ursachencode: 2581
```

2. Überprüfen Sie die Datei db2diag.log, in der Sie Status- und Fehlernachrichten finden können. Ein Teil der Datei db2diag.log wird in dem folgenden Beispiel gezeigt:

```
2009-02-10-09.49.00.660000-300 E8120712F500       LEVEL: Info
PID     : 4608                 TID  : 3956        PROC : db2syscs.exe
INSTANCE: SERVER1              NODE : 000         DB   : TSMDB1
APPHDL  : 0-7                  APPID: *LOCAL.SERVER1.090210144859
```

```
AUTHID  : B1JRPM01
EDUID   : 3956                 EDUNAME: db2agent (TSMDB1)
FUNCTION: DB2 UDB, database utilities, sqludPrintStartingMsg, probe:1292
DATA #1 : <preformatted>
Datenbankgesamtzurückschreibung wird gestartet.
Agent EDU ID: 3956

2009-02-10-09.50.21.051000-300 E8123213F483       LEVEL: Severe
PID     : 4608                 TID  : 5080        PROC : db2syscs.exe
INSTANCE: SERVER1              NODE : 000
EDUID   : 5080                 EDUNAME: db2bm.3956.1 (TSMDB1)
FUNCTION: DB2 UDB, database utilities, sqluWriteLogFile, probe:1498
MESSAGE : ZRC=0x850F000C=-2062614516=SQLO_DISK "Platte voll."
            DIA8312C Platte war voll.
DATA #1 : String, 46 bytes
F:\tivoli\tsm\Beta\sarch\RstDbLog\S0000262.LOG

2009-02-10-09.50.21.051000-300 E8124165F912       LEVEL: Severe
PID     : 4608                 TID  : 5080        PROC : db2syscs.exe
INSTANCE: SERVER1              NODE : 000
EDUID   : 5080                 EDUNAME: db2bm.3956.1 (TSMDB1)
FUNCTION: DB2 UDB, database utilities, sqluWriteLogFile, probe:1500
MESSAGE : SQL2581N  Der Restore kann keine Protokolldateien aus dem Backup-Image
          in den angegebenen Pfad extrahieren bzw. für ein Protokollverzeichnis
          kein Restore aus dem Backup-Image in den angegebenen Pfad durchführen.
          Ursachencode: "".
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:
```

Das vorherige Beispiel gibt für die Nachricht „Platte voll" an, dass nicht genügend Plattenspeicherplatz verfügbar war, um die erforderlichen Protokolldateien für die Sicherungsoperation zu speichern.

3. Fügen Sie Plattenspeicherplatz hinzu und führen Sie die Operation erneut aus.

Allgemeine Fehler bei BACKUP DB und RESTORE DB

Allgemeine Fehler, die von den Befehlen **BACKUP DB** und **RESTORE DB** abgeleitet werden, können SQL-Rückkehrcodes oder -Fehlercodes einschließen.

Die folgenden Fehler sind einige allgemeine Fehler, die angezeigt werden können, wenn die Befehle **BACKUP DB** und **RESTORE DB** ausgegeben werden.

ANR2968E - Datenbanksicherung beendet. DB2-SQLCODE: -2033, SQL-Fehlernachrichtencode: 406

Damit die SQL-Fehlernachricht 406 aufgelöst wird, muss Folgendes sichergestellt sein:

- Die Umgebungsvariable DSMI_CONFIG verweist auf eine gültige IBM Spectrum Protect-Optionsdatei.
- Der Instanzeigner hat Lesezugriff auf die Datei `dsm.opt`.
- Die Umgebungsvariable DSMI_CONFIG ist in `~/sqllib/userprofile` und in `~/sqllib/usercshrc` definiert.

DB2-SQLCODE: -2033, DB2-SQL-Fehlernachrichtencode: 106

Falls Sie die SQL-Fehlernachricht 106 empfangen, kann dies bedeuten, dass ein Berechtigungsproblem für die Protokolldatei besteht, die von der Anwendungsprogrammierschnittstelle (API) für den Client geschrieben wird.

Um den Fehler zu beheben, suchen Sie die Protokolldatei mit dem Berechtigungsproblem, melden Sie sich mit der Rootbenutzer-ID an und löschen Sie die Datei.

DB2-SQLCODE: -2033, DB2-SQL-Fehlernachrichtencode: 168

Stellen Sie sicher, dass die Umgebungsvariable DSMI_DIR auf das ausführbare Client-API-Verzeichnis verweist, das den Trusted Communication Agent (`dsmtca`) enthält.

ANR2971E - Sicherung/Zurückschreibung/Rollforward der Datenbank beendet - Fehler mit DB2-SQLCODE - 2071

Die Bibliothek konnte nicht geladen werden, da sie selbst oder eine von ihr benötigte Bibliothek nicht vorhanden ist oder kein gültiges Format hat. Falls eine Bibliothek nicht geladen werden kann, bedeutet dies normalerweise, dass eine 32-Bit-Bibliothek in eine 64-Bit-Instanz oder eine 64-Bit-Bibliothek in eine 32-Bit-Instanz geladen wird. Kann eine Bibliothek nicht geladen werden, bedeutet dies auch, dass die Umgebungsvariable DSMI_DIR auf die falschen ausführbaren Dateien für die IBM Spectrum Protect-Client-API verweist. Um Informationen zum Fehler abzurufen, öffnen Sie ein Fenster des DB2-Befehlszeilenprozessors und geben Sie den folgenden Befehl aus:

```
db2 => ? sql2071
```

Wurden Änderungen an den Dateien `tsmdbmgr.opt`, `dsm.sys` und `sqllib/userprofile` vorgenommen, stellen Sie sicher, dass die DB2-Instanz erneut gestartet wird, damit die neuen Werte berücksichtigt werden. Um die DB2-Instanz erneut zu starten, stoppen und starten Sie den IBM Spectrum Protect-Server. Stellen Sie außerdem sicher, dass der Befehl **`EXPORT`** vor den Einträgen `DSMI_*=` in der Datei `sqllib/userprofile` steht.

Fehlernachricht gibt an, dass der Knoten gesperrt ist

Möglicherweise empfangen Sie einen Fehler, wenn DB2 den Server und einen bestimmten Knoten anspricht, aber die Fehlernachricht empfängt, dass der Knoten gesperrt ist.

Um den Fehler zu beheben, verwenden Sie die Adresse des lokalen Hosts (localhost) anstelle einer expliziten Loopback-Adresse (z. B. 127.0.0.1). Geben Sie hierzu die Option `tcpserveraddress localhost` in der Zeilengruppe SERVERNAME TSMDBMGR_TSMINST1 der Datei `dsm.sys` an.

Leistungsprobleme bei der Datenbanksicherung

In manchen Fällen kann es sein, dass Datenbanksicherungen nur langsam ausgeführt werden. Dies gilt insbesondere bei AIX-Systemen, falls der Server zur Verwendung von TCP/IP für Datenbanksicherungs- und -zurückschreibungsoperationen konfiguriert ist. Konfigurieren Sie zur Problemlösung die Serverinstanz so, dass stattdessen gemeinsam genutzter Speicher verwendet wird.

Zugehörige Tasks:

„Serverinstanz für die Verwendung von gemeinsam genutztem Speicher konfigurieren” auf Seite 60

Merkmale der Benutzer-ID $$_TSMDBMGR_$$

Der IBM Spectrum Protect-Server generiert beim Start die Benutzer-ID $$_TSMDBMGR_$$.

Sie können die Benutzer-ID $$_TSMDBMGR_$$ mit einem Befehl **QUERY SESSION** anzeigen. Diese ID wird auch in der Aktivitätenprotokolldatei und in anderen Serverprotokolldateien angezeigt.

Der Server verwendet die Benutzer-ID $$_TSMDBMGR_$$, um die Serverdatenbank zu sichern. Durch die Verwendung der Benutzer-ID $$_TSMDBMGR_$$ können Sie die Datenbank für die Verarbeitung zugänglich machen, wenn der Server nicht verfügbar ist. Die Änderung dieser ID kann zur Folge haben, dass ein Server im Katastrophenfall nicht wiederhergestellt oder zurückgeschrieben werden kann.

Einschränkung: Sie können die Datei `dsm.sys` oder `dsm.opt` nicht ändern, um einen anderen Clientknotennamen zu definieren oder zu verwenden. Die lokale IBM Spectrum Protect-Serverdatenbank verwendet die Datei `dsm.sys` oder `dsm.opt`, um die eigene Datenbank zu sichern.

Probleme bei der Datenbankreorganisation beheben

Die Datenbanktabellen- und Indexreorganisation erfordern in hohem Maße Systemressourcen. Um zu vermeiden, dass Systemressourcen belegt werden, die an anderer Stelle verwendet werden können, führen Sie Ihre Reorganisationsroutinen zu Zeiten mit geringer Auslastung aus.

Ein nicht erwartetes Datenbankwachstum und ein nicht erwarteter Speicherbedarf für aktive Protokolldateien und Archivprotokolle können auftreten, wenn Tabellen oder Indizes, die Tabellen zugeordnet sind, nicht reorganisiert werden. Tabellen werden von IBM Spectrum Protect standardmäßig reorganisiert. Wenn die automatische Reorganisation Auswirkungen auf die Serverleistung hat, können Sie die Reorganisation manuell planen.

Die folgenden Vorschläge können Ihnen bei der Konfiguration der Reorganisation helfen:

- Aktivieren Sie die Indexreorganisation, wenn Sie die Deduplizierung auf Ihrem Server ausführen. Siehe die Serveroption `ALLOWREORGINDEX`.
- Standardmäßig ist die Tabellenreorganisation 24 Stunden aktiviert. Führen Sie die Reorganisation zu einer Zeit mit geringer Auslastung während des Tages aus. Zum Definieren einer Leerlaufzeit, in der die Reorganisation ausgeführt werden kann, siehe die folgenden Serveroptionen:
  - `REORGBEGINTIME`
  - `REORGDURATION`

Prozesssymptome zur Behebung von Problemen analysieren

Sie können manchmal die Fehlerursache bestimmen, indem Sie die Prozesssymptome beobachten.

Sie können eines der folgenden Prozesssymptome feststellen:

- Unzureichender Speicherbereich in einem Kopienzielspeicherpool
- Beschädigte Datei auf einem Datenträger gefunden
- Dateien verfallen nicht nach der Verringerung der Anzahl der Versionen, die aufbewahrt werden müssen
- Umlagerung wird für Speicherpool für sequenzielle Datenträger nicht ausgeführt
- Umlagerung verwendet nur einen Prozess
- Ausführung des Prozesses erfolgt langsam

Prozessnachrichten überprüfen, um den Status von Serveroperationen zu bestimmen

Serverprozesse geben unabhängig davon, ob sie im Vordergrund oder Hintergrund ausgeführt werden, neben den allgemeinen Prozessnachrichten immer eine Nachricht „Prozess gestartet" und eine Nachricht „Prozess beendet" aus. Sie können diese Nachrichten verwenden, um den Status Ihrer Serveroperation zu bestimmen.

Prozesse, die auf dem Server ausgeführt werden

Ein Serverprozess ist eine Task, die auf dem Server ausgeführt wird. Sie können die Task zuordnen, um eine bestimmte Operation auszuführen, wie z. B. Umlagerung von Daten aus einem Speicherpool in den nächsten Speicherpool in der Hierarchie. Verwenden Sie die Serverprozesse, um Probleme zu beheben, die Sie mit Ihrem Server haben.

Ein Serverprozess wird normalerweise als automatisierter Prozess auf dem Server eingeleitet. Der Prozess kann durch eine Serveroption oder eine andere Einstellung beeinflusst werden. Der Serverprozess kann auch durch einen Befehl gestartet werden.

Viele Serverprozesse können im Vordergrund (FOREGROUND) oder synchron ausgeführt werden. Prozesse, die im Vordergrund ausgeführt werden, können durch einen Befehl mit dem Parameter WAIT=YES eingeleitet werden. Befehle, mit denen Serverprozesse gestartet werden, die den Parameter WAIT=YES nicht zulassen, oder Befehle, die mit WAIT=NO angegeben werden, werden im Hintergrund (BACKGROUND) oder asynchron ausgeführt.

Einige Serverprozesse können viele Prozesse gleichzeitig einleiten, um die Task auszuführen. Siehe Tabelle 7 für Beschreibungen der Serverprozesse.

Tabelle 7. Serverprozesse

Prozess oder Befehl	Beschreibung	Wird im Vordergrund oder als Mehrfachprozess ausgeführt
AUDIT VOLUME	Den Inhalt eines Datenträgers überprüfen, um zu bestimmen, ob die Daten noch gelesen werden können und die Serverdatenbankdefinitionen, die die Daten beschreiben, korrekt sind.	

Tabelle 7. Serverprozesse (Forts.)

Prozess oder Befehl	Beschreibung	Wird im Vordergrund oder als Mehrfachprozess ausgeführt
BACKUP DB	Die Serverdatenbank sichern (FULL oder INCREMENTAL).	BACKUP DB kann als synchroner Prozess ausgeführt werden, indem WAIT=YES angegeben wird.
BACKUP STGPOOL	Einen primären Serverspeicherpool in einen Kopienspeicherpool sichern. Als Ergebnis können Sie Duplikatkopien der Daten erstellen und die Duplikatkopien an einem anderen Standort aufbewahren.	**BACKUP STGPOOL** kann als synchroner Prozess ausgeführt werden, indem **WAIT=YES** angegeben wird. **BACKUP STGPOOL** kann unter Verwendung mehrerer gleichzeitig ablaufender Prozesse ausgeführt werden. Dies wird durch den Parameter **MAXPROCESS** gesteuert, der im Befehl **BACKUP STGPOOL** angegeben wird.
CHECKIN LIBVOLUME	Einen Banddatenträger in ein Bandarchiv zurückstellen.	
CHECKOUT LIBVOLUME	Einen Banddatenträger aus einem Bandarchiv entnehmen.	
Expiration	Clientsicherungs- und -archivierungsdateien auf der Basis der Maßnahmen, die für die Verwaltung dieser Dateien definiert wurden, auf dem Server löschen. Sie können die Verfallsverarbeitung automatisch ausführen, indem Sie EXPINTERVAL=*n* in der Serveroptionsdatei angeben. Dabei ist *n* eine beliebige Zahl außer Null. Die Verfallsverarbeitung kann auch mit dem Befehl **EXPIRE INVENTORY** eingeleitet werden. Es ist nicht möglich, mehrere Verfallsprozesse gleichzeitig auszuführen, obwohl Sie mehrere Threads gleichzeitig ausführen können.	Der Befehl **EXPIRATION** kann als synchroner Prozess ausgeführt werden, indem WAIT=YES angegeben wird.
IMPORT	Daten von sequenziellen Datenträgern oder direkt von einem anderen Server unter Verwendung von TCP/IP-DFV-Verbindungen zwischen den Servern importieren. Die Importverarbeitung kann mit einem der folgenden Befehle gestartet werden: • **IMPORT ADMIN** • **IMPORT NODE** • **IMPORT POLICY** • **IMPORT SERVER**	

Tabelle 7. Serverprozesse (Forts.)

Prozess oder Befehl	Beschreibung	Wird im Vordergrund oder als Mehrfachprozess ausgeführt
LABEL LIBVOLUME	Einen oder mehrere Datenträger in einem Kassettenarchiv mit einem Kennsatz versehen.	
Migration	Daten aus einem Speicherpool in den nächsten Speicherpool in der Speicherhierarchie umlagern. Die Umlagerung wird auf der Basis der oberen und unteren Umlagerungsschwellenwerte, die für den Speicherpool definiert sind, gestartet und gestoppt. Bei jeder Ausgabe von **UPDATE STGPOOL** werden diese Werte erneut überprüft und wird, falls zutreffend, **MIGRATION** gestartet. Andernfalls überwacht der Server den Auslastungsgrad für nicht umgelagerte Daten in einem Speicherpool. Falls erforderlich, startet der Server die Umlagerungsverarbeitung für diesen Speicherpool, wenn der obere Umlagerungsschwellenwert überschritten wird. Sie können auch den Befehl **MIGRATE STGPOOL** ausgeben, um die Umlagerungsverarbeitung manuell zu starten.	Die Umlagerung kann so konfiguriert werden, dass mehrere gleichzeitig ablaufende Prozesse ausgeführt werden. Mehrere Prozesse werden durch das Attribut MIGPROCESS des Speicherpools gesteuert und können mit dem Befehl **UPDATE STGPOOL** aktualisiert werden.
MOVE DATA	Daten von einem Datenträger auf andere Datenträger in demselben Speicherpool oder in einem anderen Speicherpool versetzen.	Der Befehl **MOVE DATA** kann als synchroner Prozess ausgeführt werden, indem `WAIT=YES` angegeben wird.
MOVE DRMEDIA	Die Datenträger zur Wiederherstellung nach einem Katastrophenfall verwalten, indem die Datenträger vor Ort an einen anderen Standort versetzt werden oder die Datenträger an einem anderen Standort wieder vor Ort gebracht werden. Datenträger zur Wiederherstellung nach einem Katastrophenfall sind die Datenbanksicherungs- und Speicherpoolsicherungsdatenträger, die zum Schützen und Wiederherstellen des Servers erforderlich sind.	Der Befehl **MOVE DRMEDIA** kann als synchroner Prozess ausgeführt werden, indem `WAIT=YES` angegeben wird.
MOVE MEDIA	Datenträger aus einem Bandarchiv an den Überlaufstandort versetzen, um zu verhindern, dass ein Archiv voll wird.	
MOVE NODEDATA	Alle Daten für den oder die angegebenen Knoten auf andere Datenträger in demselben Speicherpool oder in einem anderen Speicherpool versetzen.	Der Befehl **MOVE NODEDATA** kann als synchroner Prozess ausgeführt werden, indem `WAIT=YES` angegeben wird.

Tabelle 7. Serverprozesse (Forts.)

Prozess oder Befehl	Beschreibung	Wird im Vordergrund oder als Mehrfachprozess ausgeführt
PREPARE	Eine Wiederherstellungsplandatei erstellen.	Der Befehl **PREPARE** kann als synchroner Prozess ausgeführt werden, indem WAIT=YES angegeben wird.
Reclamation	Speicherbereich von Banddatenträgern zurückfordern, indem aktive Daten auf andere Datenträger versetzt werden und die Datenträger wieder in den Status 'leer' und 'privat' oder andernfalls in den Status 'Arbeitsdatenträger' versetzt werden. Der Server überwacht den Wiederherstellungsschwellenwert (**RECLAMATION THRESHOLD**), der für einen Speicherpool definiert ist. Wenn der Server bestimmt, dass ein oder mehrere auswählbare Datenträger vorhanden sind, startet er einen Prozess zur Speicherbereichswiederherstellung für diesen Speicherpool, um alle auswählbaren Datenträger zurückzufordern.	
RESTORE STGPOOL	Alle Dateien für einen bestimmten Speicherpool aus einem Kopienspeicherpool zurückschreiben.	**RESTORE STGPOOL** kann als synchroner Prozess ausgeführt werden, indem WAIT=YES angegeben wird. **RESTORE STGPOOL** kann unter Verwendung mehrerer gleichzeitig ablaufender Prozesse ausgeführt werden. Dies wird durch den Parameter **MAXPROCESS** gesteuert, der im Befehl **RESTORE STGPOOL** angegeben wird.
RESTORE VOLUME	Alle Dateien für einen bestimmten Datenträger aus einem Kopienspeicherpool zurückschreiben.	Der Befehl **RESTORE VOLUME** kann als synchroner Prozess ausgeführt werden, indem WAIT=YES angegeben wird. **RESTORE VOLUME** kann unter Verwendung mehrerer gleichzeitig ablaufender Prozesse ausgeführt werden. Dies wird durch den Parameter **MAXPROCESS** gesteuert, der im Befehl **RESTORE VOLUME** angegeben wird.

Nachrichten, die beim Start von Prozessen ausgegeben werden

Wenn der Server Tasks als Prozesse ausführt, wird den Prozessen eine Identifikationsnachricht zugeordnet, mit der zurückgemeldet wird, dass sie gestartet wurden.

Der zurückgemeldete Start wird in der folgenden Nachricht ausgegeben:

```
ANR0984I Prozess Prozess-ID für Prozessname
im Prozessstatus um Zeit gestartet.
```

Die folgende Liste definiert die Variablen in dieser Nachricht:

Prozess-ID
Die numerische Prozess-ID.

Prozessname
Der Name des Prozesses.

Prozessstatus
FOREGROUND oder **BACKGROUND**. Wenn der Prozess im Vordergrund ausgeführt wird, wurde der Befehl mit dem Parameter **WAIT=YES** ausgegeben. Die Verarbeitung im Vordergrund bewirkt, dass die Verwaltungssitzung, die den Befehl ausgegeben hat, wartet, bis die Verarbeitung abgeschlossen ist. Ein Prozess, der im Hintergrund ausgeführt wird, kehrt unverzüglich zu der Verwaltungssitzung zurück, die den Befehl ausgegeben hat, und gibt an, dass ein Prozess gestartet wurde, während der Prozess noch ausgeführt wird. Prozesse, die im Hintergrund ausgeführt werden, können mit dem Befehl **QUERY PROCESS** überwacht werden.

Zeit Die Zeit, zu der der Prozess gestartet wurde.

Nachrichten, die am Ende von Prozessen ausgegeben werden

Wenn der Server Tasks als Prozesse ausführt, melden die Prozesse ihr Ende zurück. Die Nachrichten „Prozess beendet", die ausgegeben werden, variieren von Prozess zu Prozess. Die Nachricht ist davon abhängig, ob der Prozess Informationen zurückmelden muss, dass Elemente und Byte verarbeitet wurden, keine Elemente oder Byte verarbeitet wurden, Elemente verarbeitet wurden oder nur Byte verarbeitet wurden.

Prozess beendet

Wenn ein Prozess beendet wird und die Byte oder die Anzahl Dateien vom Prozess nicht zurückgemeldet werden müssen, wird die folgende Nachricht ausgegeben:

```
ANR0985I Prozess Prozess-ID für
Prozessname, der im Prozessstatus ausgeführt wird,
mit Beendigungsstatus Beendigungsstatus um Zeit beendet.
```

Die folgende Liste definiert die Variablen in dieser Nachricht:

Prozess-ID
Die numerische Prozess-ID.

Prozessname
Der Name des Prozesses.

Prozessstatus
FOREGROUND oder **BACKGROUND**. Wenn der Prozess im Vordergrund ausgeführt wird, wurde der Befehl mit dem Parameter **WAIT=YES** ausgegeben. Die Verarbeitung im Vordergrund bewirkt, dass die Verwaltungssitzung, die den Befehl ausgegeben hat, wartet, bis die Verarbeitung abgeschlossen ist. Ein Prozess, der im Hintergrund ausgeführt wird, kehrt unverzüglich zu der Verwaltungssitzung zurück, die den Befehl ausgegeben hat, und gibt an,

dass ein Prozess gestartet wurde, während der Prozess noch ausgeführt wird. Prozesse, die im Hintergrund ausgeführt werden, können mit dem Befehl **QUERY PROCESS** überwacht werden.

Beendigungsstatus
SUCCESS oder FAILURE

Zeit Die Zeit, zu der der Prozess gestartet wurde.

Prozess mit Elementen und Byte beendet

Wenn ein Prozess beendet wird und die verarbeiteten Byte und Elemente zurückgemeldet werden müssen, wird die folgende Nachricht ausgegeben:

```
ANR0986I Prozess Prozess-ID für Prozessname,
der im Status Prozessstatus ausgeführt wird, hat Anzahl Elemente
Elemente mit insgesamt verarbeitete Byte Byte mit Beendigungsstatus
Beendigungsstatus um Zeit verarbeitet.
```

Die folgende Liste definiert die Variablen in dieser Nachricht:

Prozess-ID
Die numerische Prozess-ID.

Prozessname
Der Name des Prozesses.

Prozessstatus
FOREGROUND oder **BACKGROUND**. Wenn der Prozess im Vordergrund ausgeführt wird, wurde der Befehl mit dem Parameter **WAIT=YES** ausgegeben. Die Verarbeitung im Vordergrund bewirkt, dass die Verwaltungssitzung, die den Befehl ausgegeben hat, wartet, bis die Verarbeitung abgeschlossen ist. Ein Prozess, der im Hintergrund ausgeführt wird, kehrt unverzüglich zu der Verwaltungssitzung zurück, die den Befehl ausgegeben hat, und gibt an, dass ein Prozess gestartet wurde, während der Prozess noch ausgeführt wird. Prozesse, die im Hintergrund ausgeführt werden, können mit dem Befehl **QUERY PROCESS** überwacht werden.

Anzahl Elemente
Die Anzahl der verarbeiteten Elemente.

Verarbeitete Byte
Die Anzahl der verarbeiteten Byte.

Beendigungsstatus
SUCCESS oder FAILURE

Zeit Die Zeit, zu der der Prozess gestartet wurde.

Prozess mit Elementen beendet

Wenn ein Prozess beendet wird und die verarbeiteten Elemente zurückgemeldet werden müssen, wird die folgende Nachricht ausgegeben:

```
ANR0987I Prozess Prozess-ID für Prozessname,
der im Status Prozessstatus ausgeführt wird, hat Anzahl Elemente
Elemente mit Beendigungsstatus Beendigungsstatus um Zeit verarbeitet.
```

Die folgende Liste definiert die Variablen in dieser Nachricht:

Prozess-ID
Die numerische Prozess-ID.

Prozessname
Der Name des Prozesses.

Prozessstatus
FOREGROUND oder **BACKGROUND**. Wenn der Prozess im Vordergrund ausgeführt wird, wurde der Befehl mit dem Parameter **WAIT=YES** ausgegeben. Die Verarbeitung im Vordergrund bewirkt, dass die Verwaltungssitzung, die den Befehl ausgegeben hat, wartet, bis die Verarbeitung abgeschlossen ist. Ein Prozess, der im Hintergrund ausgeführt wird, kehrt unverzüglich zu der Verwaltungssitzung zurück, die den Befehl ausgegeben hat, und gibt an, dass ein Prozess gestartet wurde, während der Prozess noch ausgeführt wird. Prozesse, die im Hintergrund ausgeführt werden, können mit dem Befehl **QUERY PROCESS** überwacht werden.

Beendigungsstatus
SUCCESS oder FAILURE

Zeit Die Zeit, zu der der Prozess gestartet wurde.

Prozess mit Byte beendet

Wenn ein Prozess beendet wird und die verarbeiteten Byte zurückgemeldet werden müssen, wird die folgende Nachricht ausgegeben:

```
ANR0988I Prozess Prozess-ID für Prozessname,
der im Status Prozessstatus ausgeführt wird, hat verarbeitete Byte
Byte mit Beendigungsstatus Beendigungsstatus um Zeit verarbeitet.
```

Die folgende Liste definiert die Variablen in dieser Nachricht:

Prozess-ID
Die numerische Prozess-ID.

Prozessname
Der Name des Prozesses.

Prozessstatus
FOREGROUND oder **BACKGROUND**. Wenn der Prozess im Vordergrund ausgeführt wird, wurde der Befehl mit dem Parameter **WAIT=YES** ausgegeben. Die Verarbeitung im Vordergrund bewirkt, dass die Verwaltungssitzung, die den Befehl ausgegeben hat, wartet, bis die Verarbeitung abgeschlossen ist. Ein Prozess, der im Hintergrund ausgeführt wird, kehrt unverzüglich zu der Verwaltungssitzung zurück, die den Befehl ausgegeben hat, und gibt an, dass ein Prozess gestartet wurde, während der Prozess noch ausgeführt wird. Prozesse, die im Hintergrund ausgeführt werden, können mit dem Befehl **QUERY PROCESS** überwacht werden.

Verarbeitete Byte
Die Anzahl der verarbeiteten Byte.

Beendigungsstatus
SUCCESS oder FAILURE

Zeit Die Zeit, zu der der Prozess gestartet wurde.

Fehlernachricht ANR1221E analysieren

Wenn Sie die Fehlernachricht ANR1221E empfangen, liegt die Ursache in der Regel in zu wenig Speicherbereich im Zielkopienspeicherpool.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Fehlernachricht ANR1221E zu beheben:

Vorgehensweise

1. Geben Sie den Befehl **QUERY STGPOOL** *Speicherpoolname* **F=D** aus.
2. Geben Sie die folgende SQL-Anweisung SELECT von einem Verwaltungsclient aus an diesen Server aus: „`select Speicherpoolname,Einheitenklassenname,Anzahl(*) as 'VOLUMES' from volumes group by Speicherpoolname,Einheitenklassenname`".
3. Vergleichen Sie die Anzahl der von der Anweisung SELECT zurückgemeldeten Datenträger mit der maximal zulässigen Anzahl Arbeitsdatenträger (die vom Befehl **QUERY STGPOOL** zurückgemeldet wurde). Wenn die Anzahl der von der Anweisung **SELECT** zurückgemeldeten Datenträger größer-gleich dem Wert für die „maximal zulässige Anzahl Arbeitsdatenträger" ist, aktualisieren Sie den Speicherpool und erhöhen Sie den Wert für die maximal zulässige Anzahl Arbeitsdatenträger. Wenn in dem Speicherpool keine Arbeitsdatenträger verwendet werden (scratch=0), stellen Sie sicher, dass Sie weitere private Datenträger hinzufügen. Geben Sie den Befehl `UPDATE STGPOOL Speicherpoolname MAXSCR=nn` aus; dabei ist *Speicherpoolname* der Name des zu aktualisierenden Speicherpools und *nn* ist der Wert, um den die Anzahl Arbeitsdatenträger, die diesem Kopienspeicherpool zur Verfügung gestellt werden sollen, erhöht wird.

   Wichtig: Für das Bandarchiv sollte diese Anzahl zusätzlicher Arbeitsdatenträger zur Verfügung stehen; andernfalls müssen Sie dem Bandarchiv Arbeitsdatenträger hinzufügen, bevor Sie diesen Befehl ausgeben und die Operation **BACKUP STGPOOL** wiederholen.

Fehlernachricht ANR2317W analysieren

Die Fehlernachricht ANR2317W wird ausgegeben, wenn ein Prozess eine beschädigte Datei erkennt.

Informationen zu diesem Vorgang

Die Nachricht wird mit den folgenden Informationen angezeigt:

`ANR2317W Datenträgerprüfung hat beschädigte Datei auf Datenträger Datenträgername gefunden: Knoten Knotenname, Typ Dateityp, Dateibereich Dateibereichsname, FSID Dateibereichs-ID, Dateiname Dateiname ist Nummer Version von Gesamtversionen Versionen.`

Führen Sie die folgenden Schritte aus, auf die Fehlernachricht ANR2317W zu beheben:

Vorgehensweise

1. Geben Sie den Befehl **QUERY VOLUME** *Datenträgername* **F=D** aus.
2. Geben Sie die folgende SQL-Anweisung SELECT von einem Verwaltungsclient aus an diesen Server aus: „`select* from VOLHISTORY where VOLUME_NAME='Datenträgername' AND TYPE='STGNEW`". Die Ergebnisse des Befehls **QUERY VOLUME** geben an, wann zuletzt Daten auf diesen Datenträger geschrieben

wurden. Die Informationen der Operation **SELECT** geben an, wann dieser Datenträger dem Speicherpool hinzugefügt wurde. In vielen Fällen kann **AUDIT VOLUME** Dateien als beschädigt zurückmelden, da zu dem Zeitpunkt, zu dem die Daten geschrieben wurden, bei der Hardware eine Störung vorlag und die Daten nicht korrekt geschrieben wurden, obwohl dem IBM Spectrum Protect-Server gemeldet wurde, dass die Operation erfolgreich ausgeführt wurde. Infolge dieser Störung, die an der Einheit vorlag, können viele Dateien auf vielen unterschiedlichen Datenträgern betroffen sein. Führen Sie die folgenden Schritte aus, um diesen Fehler zu beheben:

a. Werten Sie die Systemfehlerprotokolle oder anderen Informationen zu diesem Laufwerk aus, um festzustellen, ob immer noch ein Fehler vorliegt. Wenn immer noch Fehler zurückgemeldet werden, müssen diese zunächst behoben werden. Arbeiten Sie zur Behebung eines Hardwareproblems mit dem Hardwarehersteller zusammen.

b. Wenn es sich bei diesem Speicherpool um eine Kopie eines Speicherpooldatenträgers handelt, löschen Sie diesen Datenträger einfach mit dem Befehl **DELETE VOLUME** *Datenträgername* **DISCARDDATA=YES**. Wenn Sie das nächste Mal eine Speicherpoolsicherung für den primären Speicherpool oder die Speicherpools ausführen, in denen diese beschädigten Daten gespeichert sind, werden die Daten wieder in diesem Kopienspeicherpool gesichert und es ist keine weitere Maßnahme erforderlich.

   - Wenn es sich bei diesem Speicherpool um einen Datenträger für primäre Speicherpools handelt und die Daten direkt auf diesen Datenträger geschrieben wurden, als die Daten vom Client gespeichert wurden, ist es wahrscheinlich, dass keine unbeschädigten Kopien der Daten auf dem Server vorhanden sind. Falls möglich, sichern Sie die Dateien erneut vom Client.
   - Wenn es sich bei diesem Speicherpool um einen Datenträger für primäre Speicherpools handelt, die Daten aber mit dem Befehl **MIGRATION**, **MOVE DATA** oder **MOVE NODEDATA** auf diesen Datenträger gestellt wurden, ist möglicherweise eine unbeschädigte Kopie der Datei auf dem Server vorhanden. Wenn der primäre Speicherpool, auf dem diese Datei gespeichert war, in einem Kopienspeicherpool gesichert wurde, bevor der Befehl **MIGRATION**, **MOVE DATA** oder **MOVE NODEDATA** ausgeführt wurde, ist möglicherweise eine unbeschädigte Datei vorhanden. Wenn eine unbeschädigte Datei vorhanden ist, geben Sie den Befehl **UPDATE VOLUME** *Datenträgername* **ACCESS=DESTROYED** und anschließend den Befehl **RESTORE VOLUME** *Datenträgername* aus, um die beschädigten Dateien für diesen Datenträger aus dem Kopienspeicherpool wiederherzustellen.

Fehlernachrichten ANR1330E und ANR1331E analysieren

Möglicherweise erhalten Sie die Fehlernachricht ANR1330E oder ANR1331E, während Daten von einem IBM Spectrum Protect-Speicherpooldatenträger gelesen werden.

Wenn der Server Daten auf einem Speicherpooldatenträger speichert, werden regelmäßig selbstbeschreibende Informationen in die Daten eingefügt. Diese Informationen werden auf ihre Gültigkeit überprüft, während der Server die Daten liest. Die Nachrichten ANR1330E und ANR1331E werden ausgegeben, wenn bei der Überprüfung festgestellt wird, dass die Informationen ungültig sind. Die Fehlernachricht ANR1330E zeigt die tatsächlichen Werte an, die gelesen wurden, und die Fehlernachricht ANR1331E zeigt die Werte an, die erwartet wurden. Der Server gibt diese Nachrichten aus folgenden Gründen aus:

- Die Hardware (Plattensubsystem und Bandlaufwerk) hat beim Lesen der Daten einen Fehler festgestellt.
- Beim Schreiben der Daten ist ein Fehler aufgetreten und die Daten sind beschädigt.
- Eine Datenbankzurückschreibungsoperation wurde ausgeführt und ein Datenträger wurde nicht entsprechend geprüft und korrigiert, sodass er mit dem Zeitpunkt der Zurückschreibung synchron ist.

Sie müssen zuerst feststellen, ob die Daten auf dem Datenträger beschädigt sind oder ob ein Fehler aufgetreten ist, als der Server die unbeschädigten Daten gelesen hat. Geben Sie den folgenden Befehl für den Datenträger aus, auf dem die Daten gespeichert sind:

```
AUDIT VOLUME FIX=NO
```

Wenn bei der Prüfung keine beschädigten Dateien zurückgemeldet werden, hat IBM Spectrum Protect die Daten, die zuvor als beschädigt zurückgemeldet wurden, erfolgreich gelesen. In diesem Fall wurde der Fehler durch eine temporäre Maschinenstörung verursacht, als der Server die Daten gelesen hat. Wird bei der Prüfung jedoch immer noch zurückgemeldet, dass die Daten beschädigt sind, müssen Sie die Ursache für die Beschädigung ermitteln.

Sie können den Fehler ignorieren, aber nur, wenn er selten auftritt. Von der Hardware wird gelegentlich beim Lesen von Daten ein Fehler festgestellt. In den meisten Fällen erkennt die Hardware, dass ein Fehler aufgetreten ist, und führt die Hardware eine Wiederherstellung durch, ohne den Fehler zurückmelden zu müssen. Es gibt jedoch Situationen, in denen die Daten aufgrund eines temporären Hardwarefehlers in einem veränderten (beschädigten) Zustand gelesen werden. Die folgende Liste definiert die Ergebnisse beim Lesen von Daten und Empfangen eines Fehlers:

Prüfung OK, Fehler beim Lesen von unbeschädigten Daten auf dem Datenträger

IBM Spectrum Protect überprüft die selbstbeschreibenden Informationen und meldet die Daten als beschädigt zurück, wenn die Daten nicht mit den erwarteten Daten übereinstimmen. In den Nachrichten ANR1330E und ANR1331E werden die Daten als beschädigt zurückgemeldet.

Werden nach der Prüfung des Datenträgers die Nachrichten ANR1330E und ANR1331E häufig angezeigt, müssen Sie ermitteln, welche Hardwareeinheit die Ursache dafür ist, dass die Daten nicht ordnungsgemäß gelesen werden. Fragen Sie das Aktivitätenprotokoll nach dem Datum und die Zeit ab, an dem bzw. zu der die Nachrichten ANR1330E und ANR1331E ausgegeben wurden, und stellen Sie die Informationen Ihrem Hardwareunterstützungsteam zur Verfügung. Mit diesen Informationen kann das Unterstützungsteam die Hardwarefehlerprotokolle auf Operationen untersuchen, die möglicherweise abnormal beendet wurden. Ihr Hardwareunterstützungsteam muss auch sicherstellen, dass die Einheitentreiber und die Mikrocodewartung für die Hardware auf dem aktuellen Stand sind.

Im Allgemeinen treten diese Fehler in einem Speicherbereichsnetz (SAN) auf. Normalerweise treten sie auf, wenn viele LLI-Fehler (LLI = Link Level Interrupt) an dem Switch oder im Netz auftreten. LLI-Fehler zeigen an, dass die Systemleistung schlecht ist, und bewirken, dass Daten während der erneuten Übertragung geändert werden. Bitten Sie Ihr Hardwareunterstützungsteam, die Netzfehlerprotokolle auf Instanzen von LLI-Fehlern zu

untersuchen. Suchen Sie nach LLI-Fehlern, die in dem Zeitraum protokolliert wurden, in dem die Nachrichten ANR1330E und ANR1331E ausgegeben wurden.

Prüfung fehlgeschlagen, Daten auf dem Datenträger sind beschädigt

Wenn bei der Prüfung die Daten als beschädigt zurückgemeldet werden, ist möglicherweise ein Fehler aufgetreten, der verursacht hat, dass die Daten nicht ordnungsgemäß auf den Datenträger geschrieben wurden. Es ist auch möglich, dass bei einer Datenbankzurückschreibungsoperation ein Datenträger verwendet wird, der nicht entsprechend geprüft und korrigiert wurde, sodass er mit dem Zeitpunkt der Zurückschreibung synchron ist. Bestimmen Sie anhand der Prüfberichte, wann die Daten geschrieben wurden, und untersuchen Sie die Nachricht ANR1331E, um festzustellen, welche Hardwareeinheit die Daten beschädigt hat. Siehe die folgenden Beispieldaten:

```
ANR1330E
Der Server hat eine mögliche Beschädigung in einem Objekt erkannt,
das zurückgeschrieben oder versetzt wird. Die tatsächlichen Werte für den
falschen Rahmen sind: Dateitypanzeiger C6A2D75D
Hdr-Version 35134 Hdr-Länge 43170 Folgenummer 160421181 Datenlänge
7E53DCD8 Server-ID 348145193 Segment-ID 327643666840426461 CRC 06E04914.

ANR1331E
Ungültigen Rahmen erkannt. Dateitypanzeiger 53454652 Folgenummer
00000023 Server-ID 00000000 Segment-ID 2062 erwartet.
```

Die Segment-ID-Nummer in der Nachricht ANR1331E lautet in diesem Beispiel 2062. Um das Datum zu bestimmen, an dem die Daten in den Server eingefügt wurden, geben Sie den folgenden Befehl aus:

```
SHOW INVO 0 2062
```

Das folgende Beispiel zeigt die Ausgabe des Befehls **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:
Expiring object entry not found.
```

Suchen Sie das Feld `Inserted` und notieren Sie das Datum und die Zeit. In diesem Beispiel wurde das Objekt am 11/29/2009 um 13:28:26 eingefügt. Stellen Sie Ihrem Hardwareunterstützungsteam das Datum und die Zeit zur Verfügung. Das Unterstützungsteam kann die Hardwarefehlerprotokolle auf Operationen untersuchen, die abnormal beendet wurden. Das Unterstützungsteam muss auch sicherstellen, dass die Einheitentreiber und die Mikrocodewartung für die Hardware auf dem aktuellen Stand sind. Ihr Hardwareunterstützungsteam muss die SAN-Netzfehlerprotokolle untersuchen. Suchen Sie nach Fehlern, die in dem Zeitraum aufgetreten sind, in dem die Daten in IBM Spectrum Protect eingefügt wurden.

Wenn der Befehl **SHOW INVO** keine hilfreiche Ausgabe zurückgibt, geben Sie den folgenden Befehl aus, um das Einfügedatum zu bestimmen:

```
SHOW BFO 0 xxx
```

Dabei ist xxx die Segmentgruppen-ID. Das Beispiel zeigt die Ausgabe des Befehls **SHOW BFO**:

```
Bitfile Object: 0.xxx
**Super-bitfile 0.xxx contains following aggregated bitfiles
(offset/length)
0.2063 0.75295 0.3071 Active
0.2064 0.78366 0.88780 Active
0.2065 0.167146 0.13831 Active
0.2066 0.180977 0.21254 Active
0.2067 0.202231 0.3808 Active
0.2068 0.206039 0.11261 Active

**Disk Bitfile Entry
Bitfile Type: PRIMARY
Storage Format: 22
Logical Size: 0.217364
Physical Size: 0.221184
Number of Segments: 1,
Deleted: False
Storage Pool ID: 1
Volume ID: 2
Volume name: TapeVol1
```

Rufen Sie die Nummer einer zusammengefassten Bitdatei aus dem ersten Eintrag in der Liste der zusammengefassten Bitdateien ab. Im vorherigen Beispiel lautet die Nummer der ersten zusammengefassten Bitdatei 2063. Geben Sie den Befehl **SHOW INVO** mit 2063 aus.

Keine Hardwarefehler zum Zeitpunkt der Einfügung

Wenn das Hardwareunterstützungsteam feststellt, dass keine Hardwarefehler zu dem Zeitpunkt aufgetreten sind, zu dem die Daten in IBM Spectrum Protect eingefügt wurden, benachrichtigen Sie das IBM Unterstützungsteam. Stellen Sie dem Team das Aktivitätenprotokoll für die Zeit zur Verfügung, zu der die Nachrichten ANR1330E und ANR1331E ausgegeben wurden. Geben Sie außerdem den Befehl **AUDIT VOLUME FIX=NO** mit dem folgenden Trace aus und stellen Sie den Trace dem IBM Spectrum Protect-Unterstützungsteam zur Verfügung:

```
TRACE ENABLE BF AF DF SS AS DS SSFRAME
TRACE DISABLE BFLOCK AFLOCK SSLOCK
TRACE BEGIN filename
```

Beschädigte Dateien auf dem Datenträger korrigieren

Wenn Sie feststellen, dass die Daten auf einem Datenträger beschädigt sind, geben Sie den Befehl **AUDIT VOLUME FIX=YES** für den Datenträger aus. Wenn die folgenden Bedingungen zutreffen, bleiben die Daten auf dem Datenträger des primären Pools als beschädigt markiert:

- Der Datenträger ist ein Datenträger des primären Pools
- Die Daten werden in einem Kopienspeicherpool gesichert
- Die Daten sind beschädigt

Nachdem der Befehl **AUDIT VOLUME FIX=YES** ausgeführt wurde, geben Sie den Befehl **RESTORE VOLUME** für den Datenträger des primären Pools aus. Die beschädigten Daten werden durch eine neue Kopie der Daten ersetzt. Wenn der Befehl **AUDIT VOLUME FIX=YES** die Daten erfolgreich gelesen hat, sind die Daten im primären Speicherpool nicht mehr als beschädigt markiert.

Ist keine Sicherungskopie vorhanden, löscht der Befehl **AUDIT VOLUME FIX=YES** die Daten. Wenn die gelöschten Daten Sicherungsdaten sind, werden sie bei der nächsten Ausführung der Clientsicherung auf den Server gestellt.

Wenn sich die Daten, die von dem Befehl **AUDIT VOLUME FIX=YES** gelöscht werden, auf einem Kopienspeicherpooldatenträger befinden, werden die Daten auf dem Kopienpooldatenträger gelöscht. Bei der nächsten Sicherung des primären Speicherpools wird dem Kopienspeicherpool eine neue Kopie hinzugefügt.

Dateien verfallen nicht nach Verringerung der Versionszahl

Sie können die Servermaßnahmen aktualisieren, um die Anzahl Versionen einer Datei, die Sie aufbewahren möchten, zu reduzieren, aber manchmal können als Ergebnis dieser Aktualisierungen Fehler generiert werden.

Geben Sie den Befehl **QUERY COPYGROUP** *Domänenname Name der Maßnahmengruppe Kopiengruppenname* **F=D** aus. Wenn der Parameter **Versionen bestehender Daten** oder **Versionen gelöschter Daten** für eine Kopiengruppe **TYPE=BACKUP** geändert wurde, kann die Verfallsverarbeitung davon betroffen sein.

Wurde der Wert für **Versionen bestehender Daten** oder **Versionen gelöschter Daten** für eine Kopiengruppe **TYPE=BACKUP** verringert, erkennt der Serververfallsprozess diese Tatsache möglicherweise nicht sofort und der Prozess lässt diese Dateien unter Umständen verfallen. Der Server wendet die Werte für **Versionen bestehender Daten** und **Versionen gelöschter Daten** auf Dateien nur bei deren Sicherung auf dem Server an. Wenn eine Datei gesichert wird, zählt der Server die Anzahl Versionen dieser Datei. Wenn diese Anzahl die Anzahl der aufzubewahrenden Versionen übersteigt, markiert der Server die ältesten Versionen, die diesen Wert übersteigen, für die Verfallsverarbeitung.

Prozesssymptome geben Umlagerungsfehler an

Prozesssymptome können auf die Umlagerung als Fehlerursache hindeuten.

Umlagerung wird für Speicherpool für sequenzielle Datenträger nicht ausgeführt

Wenn die Umlagerung für Speicherpools für sequenzielle Datenträger nicht ausgeführt wird, geben Sie den Befehl **QUERY STGPOOL** *Speicherpoolname* **F=D** aus.

Bei der Umlagerung aus Speicherpools für sequenzielle Datenträger wird „% Ausl." als Anzahl der Datenträger, die für den Speicherpool verwendet werden, in Relation zur Gesamtzahl der Datenträger, die für diesen Speicherpool verwendet werden können, berechnet. Außerdem wird „% Uml." als Anzahl der für den Speicherpool verwendeten Datenträger mit Daten, die umgelagert werden können, in Relation zur Gesamtzahl der Datenträger, die für diesen Speicherpool verwendet werden können, berechnet. Da nicht verwendete Arbeitsdatenträger bei dieser Berechnung berücksichtigt werden können, erscheinen möglicherweise nicht genügend Daten, die in dem Speicherpool umgelagert werden können, für die Umlagerungsverarbeitung vorhanden zu sein.

Umlagerung verwendet nur einen Prozess

Geben Sie den Befehl **QUERY STGPOOL** *Speicherpoolname* **F=D** und den Befehl **QUERY OCCUPANCY * * STGPOOL**= *Speicherpoolname* aus.

Nachfolgend sind die Gründe aufgelistet, warum nur ein Umlagerungsprozess ausgeführt wird:

- Die Einstellung für 'Umlagerungsprozesse' für den Speicherpool ist auf 1 gesetzt oder nicht definiert (leer). Falls zutreffend, geben Sie den Befehl **UPDATE STGPOOL** *Speicherpoolname* **MIGPROCESS**=*n* aus, wobei *n* die Anzahl der Prozesse ist, die für die Umlagerung aus diesem Pool verwendet werden sollen. Dieser Wert muss kleiner-gleich der Anzahl der Laufwerke (Grenzwert für Ladeanforderungen) für den nächsten Speicherpool sein, in dem von der Umlagerung Daten gespeichert werden.
- Wenn von dem Befehl **QUERY OCCUPANCY** nur ein einzelner Clientknoten und Dateibereich in diesem Speicherpool zurückgemeldet wird, kann die Umlagerung nur einen einzigen Prozess ausführen, auch wenn die Einstellung für 'Umlagerungsprozesse' für den Speicherpool größer als 1 ist. Bei der Umlagerungsverarbeitung werden Daten auf der Basis des Clientknotens und Dateibereichs partitioniert. Damit die Umlagerung mit mehreren Prozessen ausgeführt werden kann, müssen Daten für mehrere Clientknoten in diesem Speicherpool verfügbar sein.

Speicherpoolprobleme beheben

Speicherpools sind integraler Bestandteil einer erfolgreichen Serveroperation. Die IBM Spectrum Protect-Datenbank enthält in Speicherpools Informationen zu registrierten Clientknoten, Maßnahmen, Zeitplänen und Clientdaten.

Diese Informationen müssen verfügbar und gültig sein, damit IBM Spectrum Protect korrekt arbeitet. Speicherpoolfehler können sich auf die folgenden Probleme beziehen:

- Fehlgeschlagene Transaktionen
- Speicherpool, bei dem eine hohe Datenträgerverwendung festgestellt wird, nachdem der Wert für MAXSCRATCH erhöht wurde
- Speicherpool, für den „Collocate?=Yes" angegeben ist, aber die Datenträger enthalten dennoch Daten für viele Knoten
- Daten können nicht mit der Funktion für gleichzeitiges Schreiben oder mit dem Befehl **COPY ACTIVEDATA** in einem Pool für aktive Daten gespeichert werden

Nachricht „ANR0522W Transaktion ... fehlgeschlagen" empfangen

Die Nachricht ANR0522W wird angezeigt, wenn der Server in dem Speicherpool, der zum Speichern der Daten für den angegebenen Client vorgesehen ist, nicht genügend Speicherbereich zuordnen kann.

Informationen zu diesem Vorgang

Es gibt eine Reihe möglicher Ursache für das Knappwerden von Speicherbereich in einem Speicherpool. Führen Sie die folgenden Prozeduren aus, um den Speicherbereichszuordnungsfehler zu beheben:

Vorgehensweise

1. Geben Sie für die Datenträger in dem Speicherpool, auf den verwiesen wird, den Befehl **QUERY VOLUME** *Datenträgername* **F=D** aus. Überprüfen Sie alle Datenträger, für die nicht 'Lese-/Schreibzugriff' zurückgemeldet wurde. Ein Datenträger kann aufgrund eines Einheitenfehlers mit 'Lesezugriff' oder als 'Nicht verfügbar' markiert sein. Geben Sie, nachdem der Einheitenfehler behoben wurde, den

Befehl **UPDATE VOLUME** *Datenträgername* **ACCESS=READWRITE** aus, damit der Server diesen Datenträger auswählen und versuchen kann, Daten auf ihn zu schreiben.

2. Geben Sie für die Datenträger in dem Speicherpool, auf den verwiesen wird, den Befehl **QUERY VOLUME** *Datenträgername* aus. Bei Datenträgern, für die der Datenträgerstatus „Anstehend" zurückgemeldet wird, handelt es sich um Datenträger, die leer sind, aber auf die Wiederverwendung durch den Server warten. Die Wartezeit wird durch die Einstellung REUSEDELAY für den Speicherpool gesteuert und als „Verzögerungszeitraum für die Wiederverwendung des Datenträgers" im Befehl **QUERY STGPOOL** angezeigt. Werten Sie die Einstellung REUSEDELAY für diesen Speicherpool aus und reduzieren Sie, falls zutreffend, (auf der Basis Ihrer Datenverwaltungskriterien) diesen Wert, indem Sie den Befehl **UPDATE STGPOOL** *Speicherpoolname* **REUSEDELAY**=*nn* ausgeben; dabei ist *Speicherpoolname* der Name des Speicherpools und *nn* die neue Einstellung für die Wiederverwendungsverzögerung. Um die Daten durch Kollokation zusammenfassen zu können, muss im Zielspeicherpool genügend Speicherbereich für die Kollokationsverarbeitung zum Auswählen eines geeigneten Datenträgers vorhanden sein. Ob im Zielspeicherpool genügend Speicherbereich vorhanden ist, wird im Wesentlichen von der Anzahl Arbeitsdatenträger in einem Speicherpool beeinflusst.
3. Geben Sie den Befehl **QUERY STGPOOL F=D** aus, um zu überprüfen, ob Lese-/Schreibzugriff besteht.

Für Speicherpool wird hohe Datenträgerverwendung nach Erhöhung des Werts für MAXSCRATCH festgestellt

Für kollokierte sequenzielle Speicherpools kann die Erhöhung des Werts für **MAXSCRATCH** dazu führen, dass der Server mehr Datenträger verwendet.

Der Server verwendet in diesem Fall aufgrund der Kollokationsverarbeitung mehr Speicherpooldatenträger. Die Kollokation gruppiert Benutzerdaten für einen Clientknoten auf demselben Band. Wenn während einer Clientsicherungs- oder -archivierungsoperation keine Bänder gegenwärtig Daten für diesen Clientknoten enthalten, wählt der Server einen Arbeitsdatenträger zum Speichern der Daten aus. Anschließend wählt der Server zum Speichern von Daten für andere Clientknoten wieder einen Arbeitsdatenträger aus. Der Grund, dass Arbeitsdatenträger nicht vor der Änderung der Einstellung für **MAXSCRATCH** ausgewählt werden, liegt darin, dass die Datenträgerauswahlverarbeitung auf dem Server die Kollokationsanforderung ignoriert und die Daten auf einem verfügbaren Datenträger speichert, wenn kein Arbeitsdatenträger verfügbar ist und für diesen Clientknoten noch kein bevorzugter Datenträger zugeordnet wurde.

Speicherpool ist für die Verwendung der Kollokation definiert, aber Datenträger enthalten Daten, die nicht durch Kollokation zusammengefasst sind

Wenn für einen Speicherpool die Kollokation aktiviert ist (der Parameter **COLLOCATION** also auf GROUP, NODE oder FILESPACE gesetzt ist), kann es vorkommen, dass viele Datenträger Daten enthalten, die nicht durch Kollokation zusammengefasst sind.

Es gibt zwei mögliche Ursachen für diese Situation:

- Die Daten wurden auf Datenträgern in diesem Speicherpool gespeichert, bevor für den Speicherpool die Kollokation aktiviert wurde.

- Der Speicherpool verfügte über keine Arbeitsbänder mehr und hat Daten auf dem bestmöglichen Datenträger gespeichert, selbst wenn die Kollokationsanforderung ignoriert wurde.

Wenn Daten für mehrere Knoten auf demselben Datenträger in einem Speicherpool mit aktivierter Kollokation gespeichert werden, können Sie eine der folgenden Aktionen ausführen:

- Geben Sie den Befehl **MOVE DATA** für den oder die betroffenen Datenträger aus. Der Prozess liest die Daten von dem angegebenen Datenträger und versetzt die Daten auf einen anderen Datenträger in demselben Speicherpool, wenn eine der folgenden Bedingungen zutrifft:
  - Arbeitsdatenträger sind verfügbar.
  - Datenträger mit ausreichendem Speicherbereich sind diesem Clientknoten für die Zusammenfassung ihrer Daten durch Kollokation zugeordnet.
- Ermöglichen Sie es der Umlagerung, alle Daten aus diesem Speicherpool zu versetzen, indem Sie die Schwellenwerte für HIGHMIG und LOWMIG definieren. Wenn alle Daten in den nächsten Speicherpool umgelagert werden können, werden die Kollokationsanforderungen erfüllt, falls Folgendes zutrifft:
  - Für den nächsten Speicherpool ist die Kollokation aktiviert.
  - Der nächste Speicherpool umfasst genügend Arbeitsdatenträger.
  - Dem nächsten Speicherpool sind Datenträger zugeordnet, um die Kollokationsanforderungen zu erfüllen.
- Geben Sie den Befehl **MOVE NODEDATA** für die Clientknoten aus, deren Daten sich in diesem Speicherpool befinden. Sind Arbeitsdatenträger verfügbar oder sind diesem Clientknoten Datenträger mit genügend Speicherbereich zugeordnet, um die Daten durch Kollokation zusammenzufassen, treten die folgenden Ereignisse ein:
  - Der **MOVE NODEDATA**-Prozess liest die Daten von den Datenträgern, auf denen für diesen Knoten Daten vorhanden sind.
  - Der **MOVE NODEDATA**-Prozess versetzt die Daten auf einen oder mehrere andere Datenträger in demselben Speicherpool.

Wichtig für die Zusammenfassung der Daten durch Kollokation ist es, dass genügend Speicherbereich im Zielspeicherpool vorhanden ist, damit die Kollokationsverarbeitung einen geeigneten Datenträger auswählen kann. Im Speicherpool müssen genügend leere Datenträger vorhanden sein, damit die Kollokation einen neuen Datenträger auswählen kann. Stellen Sie sicher, dass genügend leere Datenträger verfügbar sind, statt einen Datenträger zu verwenden, der bereits Daten für einen anderen Knoten enthält. Leere Datenträger können Arbeitsdatenträger sein, falls für den Speicherpool genügend Arbeitsdatenträger definiert sind. Andernfalls können Sie die leeren Datenträger definieren, indem Sie den Befehl **DEFINE VOLUME** ausgeben.

Speicherprobleme für Pools für aktive Daten beheben

Möglicherweise treten Schwierigkeiten beim Speichern von Daten in einem Pool für aktive Daten auf, wenn die Funktion für gleichzeitiges Schreiben verwendet oder der Befehl **COPY ACTIVEDATA** ausgegeben wird.

Bevor Daten in einem Pool für aktive Daten gespeichert werden können, müssen Sie eine Maßnahme erstellen, um das Speichern von Daten in dem Pool zu ermöglichen. Der Knoten, der Eigner der Daten ist, muss einer Domäne zugeordnet werden, deren Pool für aktive Daten im Feld ACTIVEDESTINATION der Domäne auf-

gelistet ist. Geben Sie den folgenden Befehl aus, um zu bestimmen, ob der Knoten einer Domäne zugeordnet ist, die das Speichern von Daten im Pool für aktive Daten erlaubt:

```
QUERY NODE Knotenname F=D
```

Das Feld 'Name der Maßnahmendomäne' zeigt die Domäne, der der Knoten zugeordnet ist. Geben Sie den folgenden Befehl aus, um zu bestimmen, ob der Pool für aktive Daten im Feld ACTIVEDESTINATION der Domäne aufgelistet ist:

```
QUERY DOMAIN Domänenname F=D
```

Ist der Pool für aktive Daten nicht aufgelistet, geben Sie den folgenden Befehl aus, um den Pool für aktive Daten zur Liste hinzuzufügen:

```
UPDATE DOMAIN Domänenname ACTIVEDESTINATION=Name des Pools für aktive Daten
```

Tipp: Nachdem Sie den Befehl **UPDATE DOMAIN** *Domänenname* **ACTIVEDESTINATION**=*Name des Pools für aktive Daten* ausgegeben haben, sind alle der Domäne zugeordneten Knoten berechtigt, Daten in dem Pool für aktive Daten zu speichern. Sollen nicht alle der Domäne zugeordneten Knoten zum Speichern von Daten berechtigt sein, müssen Sie eine neue Domäne für die Knoten erstellen, deren Daten im Pool für aktive Daten gespeichert werden sollen, und diese Knoten der neu erstellten Domäne zuordnen.

Probleme mit Cloud-Containerspeicherpools beheben

Mit IBM Spectrum Protect können Sie Daten direkt in einem Cloud-Containerspeicherpool sichern und Daten aus einem Cloud-Containerspeicherpool zurückschreiben.

Gelegentlich können Sie Leistungsprobleme oder Einschränkungen bei Cloud-Containerspeicherpools feststellen. Weitere Informationen finden Sie in Cloud-container storage pools FAQs in IBM developerWorks.

Gehen Sie anhand der folgenden Anweisungen vor, um Probleme zu beheben und Einschränkungen zu bearbeiten:

Probleme beim Löschen von Objekten aus der Cloud

Die Leistung eines Cloud-Containerspeicherpools basiert auf der Netzverbindung zwischen dem Server und der Cloud. Abhängig vom Cloud-Provider kann das Löschen von Objekten aus dem Cloudspeicher erhebliche Zeit in Anspruch nehmen. Wenn Sie beispielsweise Swift OpenStack als Cloud-Provider verwenden, müssen Sie Cloudobjekte einzeln löschen und die Netzlatenzzeit wirkt sich auf jede Löschoperation aus. Wenn Sie viele Cloudobjekte in einer kurzen Zeit löschen müssen, stellen Sie sicher, dass IBM Spectrum Protect alle Objekte löschen kann, die in der Cloud gespeichert sind. Sie stellen möglicherweise eine schlechte Leistung fest, wenn Sie einen Off-Premises-Cloud-Provider verwenden und Sie regelmäßig große Dateibereiche aus IBM Spectrum Protect löschen.

Daten entfernen, die während einer Prüfung als beschädigt oder verwaist markiert wurden

Ein beschädigter Datenbereich ist eine Datei, die über Verweise in der Serverdatenbank verfügt, aber fehlende oder beschädigte Daten in der Cloud hat. Ein verwaister Datenbereich ist ein in einem Cloud-Service-Provider gespeichertes Objekt, das über keinen Verweis in der Serverdatenbank verfügt. Der Parameter **FORCEORPHANDBDELETE** für den Befehl **AUDIT CONTAINER** ermöglicht es dem Server, das Löschen von verwaisten Bereichen aus der

Serverdatenbank zu erzwingen, auch wenn sie nicht aus dem Cloud-Containerspeicherpool gelöscht werden. Dieser Parameter ist optional.

Leistungsprobleme beim Zurückschreiben von Dateien
Wenn Sie beim Zurückschreiben von Dateien eine schlechte Leistung feststellen, überprüfen Sie, ob die Zurückschreibungsoperation in Ihrer Umgebung verfügbar ist. Siehe Technote 1659833.

Einschränkungen bei Cloud-Containerspeicherpools
Die folgenden Funktionen sind mit Cloud-Containerspeicherpools nicht kompatibel:

- Replikation eines Cloud-Containerspeicherpools mit dem Befehl **PROTECT STGPOOL**
- Umlagerung
- Konsolidierung
- Aggregation
- Kollokation
- Operationen für gleichzeitiges Schreiben
- Speicherpoolsicherungsoperationen
- Verwendung virtueller Datenträger

Außerdem können Sie den Parameter **NEXTSTGPOOL** nicht mit dem Befehl **DEFINE STGPOOL** für einen Cloud-Containerspeicherpool oder einen Verzeichniscontainerspeicherpool verwenden, da IBM Spectrum Protect nicht bestimmen kann, wann der Cloudspeicherprovider voll ist. Verwenden Sie den Parameter **NEXTSTGPOOL** nur für die Angabe eines Speicherpools mit wahlfreiem Zugriff oder eines primären sequenziellen Speicherpools. Aus diesem Grund ist die Überlauffunktionalität für containerbasierte Speicherpools nicht verfügbar.

Keine Übernahme (Failover) durch die Cloud, wenn der lokale Speicher voll wird
Wenn Sie Speicherpoolverzeichnisse mit einem Cloud-Containerspeicherpool verwenden und die Verzeichnisse keinen freien Speicherbereich mehr enthalten, werden Sicherungsoperationen vorzeitig gestoppt. Um diese Situation zu vermeiden, ordnen Sie mehr Speicherpoolverzeichnisse zu, damit dem Speicherpool mehr lokaler Speicherbereich für Sicherungsoperationen zur Verfügung steht. Sie können auch darauf warten, dass die Daten automatisch aus den lokalen Verzeichnissen gelöscht werden, nachdem die Daten in die Cloud versetzt wurden.

Einschränkungen bei der Verwendung der Knotenreplikation mit einem Cloud-Containerspeicherpool
Sie können einen Cloud-Containerspeicherpool als Zielspeicherpool auf einem Zielreplikationsserver verwenden. Ein Cloud-Containerspeicherpool kann jedoch nicht als Quellenspeicherpool auf einem Quellenreplikationsserver verwendet werden. Um Redundanz bereitzustellen, verwenden Sie die Replikationsfunktionen, die vom Cloudspeicherprovider zur Verfügung gestellt werden.

Dateitypen, die mit Cloud-Containerspeicherpools nicht verwendet werden sollten
Vermeiden Sie bei einem Cloud-Containerspeicherpool das Speichern von Clientdatentypen, die zum Speichern von Daten in Speicherpools für austauschbare Datenträger nicht optimiert sind. Vermeiden Sie beispielsweise das Speichern von Data Protection for VMware-Steuerdateien und Data Protection for SQL-Metadatendateien (für traditionelle SQL-Sicherungen). Weitere Informationen finden Sie in den folgenden Dokumenten:

- Using tape, VTL, or container storage pools with IBM Spectrum Protect for Virtual Environments, Technote 1659833
- IT11763: METADATA CONSIDERATIONS ARE MISSING IN DATA PROTECTION FOR SQL SERVER DOCUMENTATION

Kapitel 4. Fehler bei Operations Center beheben

AIX Linux Windows

Falls im Zusammenhang mit IBM Spectrum Protect Operations Center ein Problem auftritt, das Sie nicht lösen können, finden Sie unter Umständen eine mögliche Lösung in den Beschreibungen der bekannten Probleme. Es kann eventuell auch erforderlich sein, die Protokolldateien zu überprüfen und die erweiterte Traceerstellung für Operations Center zu aktivieren.

Übersicht über Protokolldateien

AIX Linux Windows

Wenn Sie aufgrund eines Problems mit dem Operations Center den IBM Software Support benachrichtigen, werden Sie von den Mitarbeitern möglicherweise aufgefordert, ihnen Protokolldateien zu senden.

Liste mit Protokolldateien

Der IBM Software Support fordert Sie möglicherweise auf, die folgenden Protokolldateien zu senden:

- Bis zu acht Operations Center-Protokolldateien:
  - `tsm_opscntr.log`
  - `tsm_opscntr1.log`
  - `tsm_opscntr2.log`
  - `tsm_opscntr3.log`
  - `tsm_opscntr4.log`
  - `tsm_opscntr5.log`
  - `tsm_opscntr6.log`
  - `tsm_opscntr7.log`

  Es können aus folgenden Gründen mehrere Operations Center-Protokolldateien vorhanden sein:
  - Wenn das Operations Center-Protokoll bis zu 8 MB groß ist, lautet die aktuelle Version `tsm_opscntr.log`, die vorherige Version hat den Namen `tsm_opscntr1.log` und die davor vorhandene Version hat den Namen `tsm_opscntr2.log` usw.
  - Wenn das Operations Center-Protokoll größer als 8 MB ist, wird das Protokoll auf mehrere Dateien verteilt, von denen jede maximal 8 MB groß ist. Wenn das Protokoll beispielsweise 15 MB groß ist, wird es auf die Dateien `tsm_opscntr.log` und `tsm_opscntr1.log` verteilt.

  Tipp: Wenn der IBM Software Support Sie auffordert, einen erweiterten Trace für das Operations Center durchzuführen, können Sie anhand der Änderungszeiten der Dateien feststellen, welche der Operations Center-Protokolldateien während der Traceerstellung erstellt werden.
- Web-Server-Protokolldateien:
  - `console.log`
  - `messages.log`

- FFDC-Protokolldateien (FFDC - Erfassung von Fehlerdaten beim ersten Auftreten):
  - `exception_summary_`*`Datum_Zeit`*`.log`
  - `ffdc_`*`Datum_Zeit`*`.log`

Speicherposition von Protokolldateien

- Die Operations Center- und Web-Server-Protokolldateien befinden sich im folgenden Verzeichnis:

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

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

  Dabei steht *`Installationsverzeichnis`* für das Verzeichnis, in dem IBM Spectrum Protect installiert ist. Beispiel:

  AIX Linux `/opt/tivoli/tsm`

  Windows `c:\Programme\Tivoli\TSM`

  Tipp: Sie können das Operations Center-Protokoll auch im Operations Center anzeigen.
- Die FFDC-Protokolldateien befinden sich an derselben Speicherposition, aber im Unterverzeichnis `ffdc`.

Zugehörige Tasks:

„Erweiterten Trace für das Operations Center starten" auf Seite 121

Operations Center-Protokoll im Operations Center anzeigen

AIX Linux Windows

Das Operations Center-Protokoll enthält Daten aus einem Trace für Operations Center-Ereignisse. Sie können das Protokoll im Operations Center anzeigen oder Sie können in das Verzeichnis wechseln, das die Protokolldatei enthält, und die Datei öffnen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das Operations Center-Protokoll anzuzeigen, während Sie am Operations Center angemeldet sind:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Fragezeichensymbol und wählen Sie **Informationen zum Operations Center** aus.
2. Klicken Sie im angezeigten Fenster auf **Installationsdetails**.
3. Klicken Sie auf die Registerkarte **Protokoll anzeigen**.
4. Klicken Sie auf **Protokoll anzeigen**.

Zugehörige Tasks:

„Erweiterten Trace für das Operations Center starten" auf Seite 121

Alerts werden nicht unverzüglich aktualisiert

AIX Linux Windows

Wenn Sie versuchen, mehrere Alerts einem Administrator zuzuordnen oder mehrere Alerts zu schließen, werden die Alerts auf der Seite **Alerts** des Operations Center nicht sofort zugeordnet oder geschlossen.

Symptom

Tabelle 8 zeigt Beispieldaten aus einer Testumgebung, in der ein Administrator mehrere Alerts aktualisiert hat. Diese Ergebnisse weichen möglicherweise von den Ergebnissen in Ihrer Speicherumgebung ab.

Tabelle 8. Ungefähre Verzögerungszeiten bei der Aktualisierung von Alerts in einer kontrollierten Umgebung

Anzahl der aktualisierten Alerts	Verzögerung für Hub-Server-Alerts	Verzögerung für Alerts aus Peripherieservern mit IBM Spectrum Protect Version 7.1.0	Verzögerung für Alerts aus Peripherieservern mit Version 6.3.4
1	6 Sekunden	7 Sekunden	7 Sekunden
10	6 Sekunden	7 Sekunden	9 Sekunden
100	6 Sekunden	8 Sekunden	40 Sekunden
1.000	10 Sekunden	20 Sekunden	5,5 Minuten
10.000	45 Sekunden	1,25 Minuten	1 Stunde

Wenn der Administrator beispielsweise 10.000 Hub-Server-Alerts ausgewählt und auf **Schließen** geklickt hat, dauerte es ungefähr 45 Minuten, bis die Alerts geschlossen waren.

Lösung

Warten Sie, bis die Alerts aktualisiert worden sind, oder aktualisieren Sie gleichzeitig weniger Alerts. Führen Sie für Peripherieserver, die Version 6.3.4 ausführen, ein Upgrade auf Version 7.1 oder höher aus.

Aktive Tasks werden nicht unverzüglich abgebrochen

AIX Linux Windows

Wenn Sie auf der Seite **Aktive Tasks** des Operations Center mehrere Tasks auswählen, und versuchen, die Tasks abzubrechen, werden die Tasks nicht sofort abgebrochen. Die Verzögerung ist für Tasks von Peripherieservern länger als für Tasks von Hub-Servern.

Symptom

Tabelle 9 auf Seite 110 zeigt Beispieldaten aus einer Testumgebung, in der ein Administrator mehrere Tasks abgebrochen hat. Diese Ergebnisse weichen möglicherweise von den Ergebnissen in Ihrer Speicherumgebung ab.

Tabelle 9. Ungefähre Verzögerungszeiten beim Abbruch von Tasks in einer kontrollierten Umgebung

Anzahl der abgebrochenen Tasks	Verzögerung für Hub-Server-Task	Verzögerung für Peripherieserver-Task
1	5 Sekunden	5 Sekunden
10	5 Sekunden	7 Sekunden
100	10 Sekunden	25 Sekunden
1000	40 Sekunden	3,5 Minuten

Wenn der Administrator beispielsweise 1.000 Hub-Server-Tasks ausgewählt und auf **Abbrechen** geklickt hat, dauerte es ungefähr 40 Sekunden, bis die Tasks abgebrochen wurden.

Lösung

Warten Sie, bis die Tasks abgebrochen wurden, oder brechen Sie gleichzeitig weniger Tasks ab.

Weitere bekannte Probleme bei Operations Center

AIX Linux Windows

Bekannte Probleme sind in der Wissensdatenbank des IBM Software Support als Technotes dokumentiert. Sobald Probleme erkannt und gelöst werden, wird die Wissensdatenbank vom IBM Software Support aktualisiert. Durch eine Suche in der Wissensdatenbank können Sie schnell Ausweichmaßnahmen oder Lösungen für Probleme ermitteln.

- Eine Liste der bekannten Probleme finden Sie in der Wissensdatenbank des IBM Software Support auf der folgenden Webseite: Bekannte Probleme im IBM Spectrum Protect Operations Center.
- Informationen zu weiteren Problemen, die erst nach dem Produktrelease bekannt wurden, finden Sie in den folgenden Suchergebnissen: Suchergebnisse für bekannte Probleme im IBM Spectrum Protect Operations Center.

Kapitel 5. Kommunikationsfehler beheben

Die Notwendigkeit der Konnektivität in IBM Spectrum Protect bedeutet, dass jeder Kommunikationsfehler Ihre Anwendung nutzlos machen kann. Kommunikationsfehler können sich auf die TCP/IP-Konfiguration oder auf Client- und Serververbindungen beziehen und andere Ursachen haben.

Beim Herstellen der Verbindung zum Server aufgetretene Fehler beheben

Fehler, die bei der Herstellung der Verbindung zum Server generiert werden, können sich auf Ihre Übertragungsoptionen beziehen.

Um den Fehler zu korrigieren, führen Sie einen oder alle aufgeführten Schritte aus:

- Überprüfen Sie die Änderungen (sofern vorhanden) an den Clientübertragungsoptionen in der Clientoptionsdatei und versuchen Sie die Werte wieder auf die vorherigen Werte zurückzusetzen. Wiederholen Sie den Verbindungsaufbau.
- Wenn die Serverübertragungseinstellungen geändert wurden, aktualisieren Sie entweder die Clientübertragungsoptionen, damit sie die geänderten Serverwerte widerspiegeln, oder setzen Sie den Server auf seine ursprünglichen Werte zurück.
- Wurden Netzeinstellungen geändert, wie z. B. die TCP/IP-Adresse für den Client oder Server (oder eine Firewall), aktualisieren Sie mit dem Netzadministrator den Client und/oder Server für diese Netzänderungen.

Unterbrochene Verbindungen durch Clients oder Administratoren beheben

Die beiden Hauptursachen für Verbindungsfehler sind allgemeine Fehler, bei denen keine Verbindungen zulässig sind, oder isolierte Fehler, bei denen einige Verbindungen zulässig sind, aber andere Verbindungen fehlschlagen.

Wenn kein Verbindungsaufbau möglich ist, müssen Sie unter Umständen den Server im Vordergrund ausführen, damit eine Serverkonsole verfügbar ist und zusätzliche Diagnoseschritte ausgeführt werden können. Überprüfen Sie die Einstellungen, um die ordnungsgemäße Konfiguration für die Kommunikation mit dem Server sicherzustellen:

- Stellen Sie sicher, dass der Server eine Bindung an einen Anschluss herstellen kann, wenn er gestartet wird. Kann der Server keine Bindung an einen Anschluss herstellen, wird dieser Anschluss wahrscheinlich von einer anderen Anwendung verwendet. Der Server kann keine Bindung an einen bestimmten TCP/IP-Anschluss herstellen (den Anschluss nicht verwenden), wenn eine andere Anwendung bereits an diesen Anschluss gebunden ist. Wenn der Server für die TCP/IP-Kommunikation konfiguriert ist und beim Start von Clientsitzungen erfolgreich eine Bindung an einen Anschluss herstellen kann, wird die folgende Nachricht ausgegeben:

  ```
  ANR8200I Der TCP/IP-Treiber
  ist für Verbindungen mit Clients am Anschluss 1500 bereit.
  ```

Wenn eine bestimmte Übertragungsmethode in der Serveroptionsdatei konfiguriert ist, aber während des Serverstarts keine Nachricht für erfolgreiches Binden ausgegeben wird, liegt ein Initialisierungsproblem bei dieser Übertragungsmethode vor.

- Stellen Sie sicher, dass die Codeeinstellung für **TCPPORT** in der Serveroptionsdatei korrekt ist. Wird die Codeeinstellung versehentlich geändert, können die Clients keine Verbindung herstellen. Der Grund ist, dass die Clients versuchen, eine Verbindung zu einem anderen TCP/IP-Anschluss als dem Anschluss herzustellen, an dem der Server empfangsbereit ist.
- Wenn mehrere Server dieselbe TCP/IP-Adresse verwenden, stellen Sie sicher, dass **TCPPORT** und **TCPADMINPORT** für jeden Server eindeutig sind. Beispiel: Zwei Server haben dieselbe TCP/IP-Adresse. Der erste Server hat **TCPPORT** mit dem Wert 1500 und **TCPADMINPORT** mit dem Wert 1500. Der zweite Server hat **TCPPORT** mit dem Wert 1501 und **TCPADMINPORT** mit dem Wert 1500. Um den Anschluss 1500 zu verwenden, sperrt der erste Server den anderen Server für den Anschluss 1500, und die Clients können nicht mehr auf den ersten Server zugreifen. Verwaltungsclients stellen immer die Verbindung zum zweiten Server her. Eine bessere Auswahl der Anschlüsse für jeden Server wäre 1500 und 1501 für TCPPORT sowie 1510 und 1511 für **TCPADMINPORT**.
- Überprüfen Sie, ob der Server für Sitzungen aktiviert ist. Geben Sie den Befehl **QUERY STATUS** aus und stellen Sie sicher, dass „Verfügbarkeit: Aktiviert" definiert ist. Lautet das Ergebnis „Verfügbarkeit: Inaktiviert", geben Sie den Befehl **ENABLE SESSIONS** aus.
- Wenn bestimmte Clients keine Verbindung zum Server herstellen können, überprüfen Sie die Übertragungseinstellungen für diese Clients. Überprüfen Sie für TCP/IP die Optionen TCPSERVERADDRESS und **TCPSERVERPORT** in der Clientoptionsdatei.
- Wird nur ein bestimmter Knoten vom Server zurückgewiesen, stellen Sie sicher, dass der Knoten auf dem Server nicht gesperrt ist. Geben Sie den Befehl **QUERY NODE** *Knotenname* aus, wobei *Knotenname* der Name des Knotens ist, der überprüft werden soll. Lautet das Ergebnis „Gesperrt?: Ja", überprüfen Sie, warum dieser Knoten gesperrt ist. Knoten können nur mit dem Verwaltungsbefehl **LOCK NODE** gesperrt werden. Wenn dieser Knoten entsperrt werden soll, geben Sie den Befehl **UNLOCK NODE** *Knotenname* aus, wobei *Knotenname* der Name des Knotens ist, der entsperrt werden soll.
- Hat der Computer, auf dem der Server ausgeführt wird, Speicher- oder Ressourcenzuordnungsprobleme, ist es unter Umständen nicht möglich, neue Verbindungen zum Server zu starten. Das Speicher- oder Ressourcenzuordnungsproblem kann temporär behoben werden, wenn Sie entweder den Server anhalten und erneut starten oder wenn Sie den Computer selbst anhalten und erneut starten. Diese Aktion ist eine temporäre Lösung und die Diagnose sollte entweder für das Betriebssystem oder den Server fortgesetzt werden, da das Speicher- und Ressourcenzuordnungsproblem auf einen Fehler im Betriebssystem oder auf dem Server hindeuten kann.

Fehler für Secure Sockets Layer beheben

SSL-Fehler (SSL = Secure Sockets Layer) können durch eine falsche Umgebungskonfiguration, ein ungültiges Serverzertifikat, Verbindungsprobleme oder Bedingungen mit fehlender Synchronisation verursacht werden oder andere Ursachen haben.

Gehen Sie anhand der folgenden Anweisungen vor, um allgemeine SSL-Probleme zwischen Client und Server sowie zwischen Server und Server zu beheben:

Keine Verbindung mit dem Server nach Verwendung eines Zertifikats eines anderen Anbieters

Wenn Sie ein Zertifikat eines anderen Anbieters verwenden und das Zertifikat nicht dem Server hinzugefügt wurde, geben Sie das Stammzertifikat in der Schlüsseldatenbank des Servers als vertrauenswürdig an. Um das Stammzertifikat der Datenbank hinzuzufügen, geben Sie den folgenden Befehl aus:

```
gsk8capicmd -cert -add -db cert.kdb -pw Kennwort
-label Name -file .der_file -format ascii
```

Das CA-Stammzertifikat wurde dem Client nicht hinzugefügt

Fügen Sie das Stammzertifikat der Schlüsseldatenbank des Clients als vertrauenswürdig hinzu:

```
gsk8capicmd -cert -add -db dsmcert.kdb -pw Kennwort
-label meine Zertifizierungsstelle -file ca.arm -format ascii
```

gsk8capicmd.exe (IBM Global Security Kit [GSKit]) kann nicht ausgeführt werden

In den meisten Fällen wird dieser Windows-Fehler durch eine falsche Umgebungskonfiguration generiert. Definieren Sie die Variable PATH wie angegeben, bevor Sie das Dienstprogramm 'gsk8capicmd' ausführen.

ANS1595E Ungültiges Serverzertifikat

Dieser Fehler wird zurückgemeldet, wenn dem Client oder Server das Serverzertifikat nicht bekannt ist. Der Fehler „Ungültiges Serverzertifikat" kann unter folgenden Bedingungen auftreten:

- Das Zertifikat wurde nie importiert
- Die Zertifikatsdatei `cert256.arm` wurde beschädigt, bevor das Zertifikat importiert wurde
- Der Befehl zum Importieren des Zertifikats wurde falsch eingegeben
- Die Variable *DSM_DIR* zeigt auf das falsche Verzeichnis, das eine falsche Schlüsseldatenbank des Clients enthält (`dsmcert.kdb`)
- Der Server ist für Transport Layer Security (TLS) 1.2 konfiguriert, aber der Client hat eine unzureichende Version (6.3 ist erforderlich)
- Der Server ist für TLS 1.2 konfiguriert, aber der Client hat die Datei `cert.arm` anstelle der Datei `cert256.arm` importiert
- Der Server ist für TLS 1.2 konfiguriert, aber der Client hat die Datei `cert256.arm` anstelle der Datei `cert.arm` importiert

Wiederholen Sie alle Schritte, die zum Importieren des Serverzertifikats erforderlich sind, und überprüfen Sie die Variable *DSM_DIR*. Weitere Informationen zu diesem Fehler finden Sie in der Datei `dsmerror.log`. Das Clientfehlerprotokoll kann ebenfalls Informationen zu einem bestimmten IBM GSKit-Fehler enthalten.

ANS1592E SSL-Protokoll konnte nicht initialisiert werden

Dieser Fehler tritt auf dem Client auf und gibt an, dass die SSL-Verbindung nicht aufgebaut wurde. Weitere Informationen zu diesem Fehler fin-

den Sie im Clientfehlerprotokoll. Der Server akzeptiert keine SSL-Sitzungen an dem Anschluss, zu dem der Client oder Server eine Verbindung herzustellen versucht. Bestimmen Sie, ob der Client oder Server auf den korrekten Serveranschluss (TCPPort) verweist, der eine andere Anschlussnummer als die Standardnummer 1500 haben kann.

ANR8583E und GSKit-Rückkehrcode 406

Dieser Fehler kann angeben, dass ein Client, der nicht für SSL aktiviert ist, versucht, einen SSL-Anschluss anzusprechen. Wenn ein Client einen Server an einem mit `SSLTCPPORT` oder `SSLTCPADMINPORT` definierten Anschluss anspricht, baut der Server eine Sitzung auf und leitet ein SSL-„Handshake" ein. Ist der Client nicht für SSL aktiviert, kann er den SSL-Handshake-Prozess nicht ausführen. Die Sitzung scheint dann gestoppt zu sein, aber ihr Zeitlimit wird durch die Option `IDLEWAIT` überschritten oder die Sitzung wird beendet, wenn der Serveradministrator den Befehl **CANCEL SESSION** ausgibt, um sie manuell abzubrechen. Das Beispiel zeigt eine Sitzung mit diesem Status auf dem Server:

```
TSM:SERVER1>query session
ANR2017I Administrator SERVER_CONSOLE hat folgenden Befehl ausgegeben: QUERY SESSION

  Sitz. Über. Sitz.  Warte- Byte    Byte    Sitz. Platt-   Client-
nummer  meth. status zeit   gesend. empf.   typ   form     name
------ ------ ------ ------ ------- ------- ----- -------- -------------
     1 SSL    IdleW   17 S        0       0 Node
```

Wichtig: Da ein gültiger Handshake-Prozess in der Systemumgebung einige Zeit in Anspruch nehmen kann, darf nicht angenommen werden, dass das Ergebnis immer einen Nicht-SSL-Client angibt.

ANR8583E und GSKit-Rückkehrcode 420 sowie ANR8581E mit GSKit-Rückkehrcode 406 treten für dieselbe IBM Spectrum Protect-Clientsitzung auf

Wenn die Servernachrichten ANR8583E und ANR8581E für dieselbe Clientsitzung angezeigt werden, hat der Client wahrscheinlich eine Nachricht ANS1595E generiert. Die Nachricht ANS1595E liegt normalerweise vor, wenn IBM Spectrum Protect versucht, eine Sitzung mit dem Server aufzubauen. Falls zutreffend, befolgen Sie die Anleitung für ANS1595E im IBM Spectrum Protect-Nachrichtenhandbuch, um diese Fehler zu beseitigen.

ANR3338E TLS weist eine frühere Version als 1.2 auf

Dieser Fehler wird zurückgemeldet, wenn der Server und der Speicheragent versuchen, eine Verbindung mit einem SSL-Protokoll herzustellen, das eine ältere Version als TLS 1.2 aufweist. Wenn für die Kommunikation zwischen Server und Speicheragent die Option `SSLDISABLELEGACYTLS` angegeben ist, müssen TLS-Sitzungen eine Verbindung mit der TLS-Mindestversion 1.2 herstellen, da die Sitzung andernfalls zurückgewiesen wird.

Überkreuzdefinition von Servern ohne SSL=YES führt zu einer Blockierung des Servers

Wenn Sie die SSL-Übertragung verwenden möchten, muss die SSL-Infrastruktur auf dem Quellen- und dem Zielreplikationsserver vorhanden sein. Erforderliche SSL-Zertifikate müssen sich in der Schlüsseldatenbankdatei befinden, die zu jedem Server gehört. Die SSL-Funktion ist aktiv, wenn die Serveroptionsdatei die Option `SSLTCPPORT` oder `SSLTCPADMINPORT` enthält oder wenn ein Server beim Start mit **SSL=YES** definiert wird.

Es erfolgt ein Eintrag, wenn ein verwendetes Zertifikat eines anderen Anbieters dem Server nicht hinzugefügt wurde oder das Zertifikat einer Zertifizierungsstelle dem Client nicht hinzugefügt wurde. Wenn eine SSL-Sitzung gestartet wird, enthält die Nachricht zum Sitzungsstart die Seriennummer aus dem Serverzertifikat. Daher kann das verwendete Zertifikat eindeutig identifiziert werden.

Zugehörige Verweise:

Anhang C, „Rückkehrcodes für IBM Global Security Kit", auf Seite 217

Kennwort für die Schlüsseldatenbankdatei wiederherstellen

Wenn Sie das aktuelle Kennwort für die Schlüsseldatenbankdatei vergessen haben, kann IBM Spectrum Protect Sie bei der Wiederherstellung des Kennworts unterstützen.

Vorbereitende Schritte

Um die Wiederherstellung des Kennworts für die Schlüsseldatenbankdatei verwalten zu können, müssen Sie über Systemberechtigungen verfügen.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um das Kennwort für die Schlüsseldatenbankdatei wiederherzustellen und zu aktualisieren:

Vorgehensweise

1. Geben Sie den Befehl **QUERY SSLKEYRINGPW** aus, um das aktuelle Kennwort für die Schlüsseldatenbank anzuzeigen.
2. Geben Sie den folgenden Befehl aus, um die Serveraufzeichnung des Kennworts für die Schlüsseldatenbank zum Aktualisieren des Kennworts zu verwenden:

   ```
   SET SSLKEYRINGPW Kennwort UPDATE=Y
   ```

   Dabei ist *Kennwort* das mit dem Befehl **QUERY SSLKEYRINGPW** abgerufene Kennwort.

Nächste Schritte

Tipp: Wenn die Datei `cert.kdb` nicht vorhanden ist, können Sie eine neue Datei erstellen, indem Sie den Server erneut starten. Der Server erstellt eine Datenbankdatei mit dem alten Kennwort und generiert beim Start ein neues selbst signiertes Zertifikat. Wenn Sie selbst signierte Zertifikate verwenden, müssen Sie das Zertifikat extrahieren und auf einem Clientsystem installieren. Wenn Sie ein Zertifikat eines anderen Anbieters verwenden, müssen Sie das Zertifikat wieder der Serverschlüsseldatenbankdatei hinzufügen und den Server erneut starten.

Fehlerbehebung für Zertifikatsschlüsseldatenbank durchführen

Sicherungskopien der Datei cert.kdb stellen sicher, dass Transport Layer Security (TLS) gestartet wird, wenn Sie einen Restore für den IBM Spectrum Protect-Server durchführen. Wenn Sie über eine Sicherungskopie verfügen, können Sie die Datei zurückschreiben und den Server erneut starten.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Sicherungskopie der Zertifikatsschlüsseldatenbank cert.kdb zu erstellen:

1. Geben Sie den Serverbefehl **DELETE KEYRING** aus, um die Kennwortinformationen in der IBM Spectrum Protect-Schlüsseldatenbank zu löschen.
2. Löschen Sie alle verbliebenen cert.*-Dateien.
3. Fahren Sie den Server herunter.
4. Starten Sie den Server. Der Server erstellt automatisch eine neue cert.kdb-Datei und einen entsprechenden Eintrag in der IBM Spectrum Protect-Datenbank. Wenn Sie den Befehl **DELETE KEYRING** nicht ausgeben, versucht der Server beim Start, die Schlüsseldatenbank mit dem vorherigen Kennwort zu erstellen.
5. Verteilen Sie die neue .arm-Datei erneut an alle Clients für Sichern/Archivieren, die TLS verwenden. Wenn Sie mit TLS 1.2 arbeiten, müssen Sie die Datei cert256.arm verwenden. Verwenden Sie die Datei cert.arm, wenn das von Ihnen verwendete TLS-Protokoll älter als 1.2 ist. Installieren Sie alle Zertifikate von Drittanbietern erneut auf dem Client für Sichern/Archivieren. Wenn Sie einen LDAP-Verzeichnisserver für die Authentifizierung von Kennwörtern verwenden, fügen Sie das Stammzertifikat hinzu, mit dem das Zertifikat des LDAP-Servers signiert wurde. Wenn es sich bei dem Stammzertifikat bereits um ein vertrauenswürdiges Standardzertifikat handelt, müssen Sie es nicht erneut hinzufügen.

Nächste Schritte

Wenn die Schlüsseldatenbankdatei cert.kdb nicht vorhanden ist, wird sie vom Server erstellt. Eine der Optionen oder beide Optionen SSLTCPPORT und SSLTCPADMINPORT müssen in der Serveroptionsdatei enthalten sein, wenn der Server gestartet wird. Der Server generiert ein änderbares Kennwort sowie ein selbst signiertes Zertifikat, das für Clients und Server von IBM Geschäftspartnern extrahiert werden kann. Wenn die Datei cert.kdb vorhanden ist oder der Server die Datei nicht erstellt hat, tritt eine Bedingung 'nicht synchron' auf, die verhindert, dass der Server die SSL-Übertragung definiert.

Kapitel 6. Speicheragentenprobleme beheben

Der kann mit dem Speicheragenten Clientdaten direkt in einem SAN-angeschlossenen Speicher sichern und von dort zurückschreiben.

Serveraktivitätenprotokoll auf Speicheragenteninformationen überprüfen

Überprüfen Sie die Serveraktivitätenprotokolldatei auf Nachrichten, die 30 Minuten vor und 30 Minuten nach dem Fehler empfangen wurden.

Speicheragenten starten und steuern viele Sitzungen für den Server. Überprüfen Sie die Serveraktivitätenprotokolldatei auf Nachrichten von dem Speicheragenten. Um die Nachrichten im Aktivitätenprotokoll zu überprüfen, geben Sie den Befehl **QUERY ACTLOG** aus.

Werden keine Nachrichten für diesen Speicheragenten in der Serveraktivitätenprotokolldatei angezeigt, überprüfen Sie die Übertragungseinstellungen:

- Geben Sie `QUERY SERVER F=D` auf dem Server aus und stellen Sie sicher, dass die Adresse der höheren Ebene (HLA) und die Adresse der unteren Ebene (LLA), die für den Servereintrag definiert sind, der diesen Speicheragenten darstellt, korrekt sind.
- Stellen Sie in der Einheitenkonfigurationsdatei, die in der Datei `dsmsta.opt` angegeben ist, sicher, dass der SERVERNAME sowie die HLA und LLA in der Zeile **DEFINE SERVER** korrekt definiert sind.

Überprüfen Sie, ob auf dem Server für diesen Speicheragenten Fehlernachrichten vorliegen.

Fehler beheben, der durch das Lesen von einer Einheit oder das Schreiben auf eine Einheit verursacht wird

Handelt es sich um einen Fehler, der beim Lesen von Daten von einer Einheit oder beim Schreiben von Daten auf eine Einheit auftritt, zeichnen viele Systeme und Einheiten Informationen in einer Systemfehlerprotokolldatei auf.

Die Systemfehlerprotokolldatei für AIX ist errpt und die Systemfehlerprotokolldatei für Windows ist das Ereignisprotokoll.

Wenn eine Einheit oder ein Datenträger, die bzw. der von IBM Spectrum Protect verwendet wird, einen Fehler an die Systemfehlerprotokolldatei zurückmeldet, handelt es sich wahrscheinlich um einen Einheitenfehler. Die in der Systemfehlerprotokolldatei aufgezeichneten Fehlernachrichten stellen möglicherweise genügend Informationen bereit, um den Fehler zu beheben.

Speicheragenten sind besonders anfällig, wenn Pfadangaben geändert werden oder nicht korrekt sind. Geben Sie den Befehl **QUERY PATH F=D** auf dem Server aus. Stellen Sie für alle Pfade des Speicheragenten sicher, dass die Einstellungen korrekt sind. Stellen Sie vor allem sicher, dass die aufgelistete Einheit mit dem Systemeinheitennamen übereinstimmt. Wenn die Pfadangaben nicht korrekt sind, aktualisieren Sie die Pfadangaben mit dem Befehl **UPDATE PATH**.

Fehler beheben, die durch die Änderung von Speicheragentenoptionen verursacht wurden

Änderungen an Optionen in der Optionsdatei des Speicheragenten können zur Folge haben, dass Operationen fehlschlagen, auch wenn sie zuvor erfolgreich ausgeführt wurden.

Überprüfen Sie alle Änderungen an der Optionsdatei des Speicheragenten. Versuchen Sie die Einstellungen auf ihre ursprünglichen Werte zurückzusetzen und wiederholen Sie die Operation. Wenn der Speicheragent jetzt ordnungsgemäß arbeitet, versuchen Sie, jeweils eine Änderung an der Optionsdatei des Speicheragenten erneut einzuführen, und wiederholen Sie die Speicheragentenoperation, bis die Änderung der Optionsdatei, die den Fehler verursacht hat, identifiziert wurde.

Fehler beheben, die durch die Änderung von Serveroptionen oder -einstellungen verursacht werden

Änderungen an Optionen in der Serveroptionsdatei oder Änderungen an Servereinstellungen mit den Befehlen **SET** können Auswirkungen auf den Speicheragenten haben.

Überprüfen Sie alle Änderungen an den Serveroptionseinstellungen. Versuchen Sie die Einstellungen auf ihre ursprünglichen Werte zurückzusetzen und wiederholen Sie die Operation. Wenn der Speicheragent jetzt ordnungsgemäß arbeitet, versuchen Sie, jeweils eine Änderung an der Optionsdatei des Speicheragenten erneut einzuführen, und wiederholen Sie die Speicheragentenoperation, bis die Änderung der Optionsdatei, die den Fehler verursacht hat, identifiziert wurde.

Überprüfen Sie die Servereinstellungen, indem Sie den Befehl **QUERY STATUS** ausgeben. Wenn Einstellungen, die von dieser Abfrage zurückgemeldet werden, geändert wurden, überprüfen Sie den Grund für die Änderung und setzen Sie (falls möglich) die Einstellung auf den ursprünglichen Wert zurück und wiederholen Sie die Speicheragentenoperation.

LAN-unabhängige Konfiguration für den Speicheragenten

Die LAN-unabhängige Datenversetzung ist das direkte Versetzen von Clientdaten zwischen einem Client-Computer und einer Speichereinheit in einem SAN anstelle eines LAN. Möglicherweise treten Probleme mit dem Speicheragenten auf, die sich auf Ihre LAN-unabhängige Konfiguration beziehen.

Problem, dass Daten direkt an den Server gesendet werden, beheben

In der Clientübersichtsstatistik sind keine Byte aufgelistet, die LAN-unabhängig übertragen wurden.

Vorbereitende Schritte

Der Client meldet die Byte zurück, die LAN-unabhängig gesendet wurden, wenn der Befehl „**ANE4971I LAN-unabhängige Datenbyte: xx KB**" ausgegeben wird. Dementsprechend meldet der Server keine Instanz von „ANR0415I Sitzung SITZUNGSNUMMER, die durch *SPEICHERAGENT* weitergeleitet wurde, wurde für

Knoten *KNOTENNAME* gestartet" für diesen Knoten und Speicheragenten zurück und gibt damit an, dass die LAN-unabhängige Weiterleitungsoperation für diesen Clientknoten ausgeführt wurde.

Der Client versucht nur, Daten LAN-unabhängig mithilfe des Speicheragenten zu senden, wenn das primäre Speicherpoolziel in der Serverspeicherhierarchie LAN-unabhängig ist. Ein Serverspeicherpool ist für einen bestimmten Speicheragenten als LAN-unabhängig aktiviert, wenn ein oder mehrere Pfade von diesem Speicheragenten zu einer SAN-Einheit definiert sind.

Informationen zu diesem Vorgang

Um zu bestimmen, ob das Speicherpoolziel korrekt konfiguriert ist, gehen Sie wie folgt vor:

Vorgehensweise

1. Geben Sie den Befehl **QUERY NODE** *Knotenname* aus, um die Maßnahmendomäne zurückzumelden, der der Knoten zugeordnet ist.
2. Geben Sie den Befehl **QUERY COPYGROUP** *Domänenname Name_der_Maßnahmengruppe Name_der_Verwaltungsklasse* **F=D** für die Verwaltungsklassen aus, die dieser Knoten von der zugeordneten Maßnahmendomäne verwenden würde. Beachten Sie, dass dieser Befehl Informationen für Sicherungsdateien zurückmeldet. Um Informationen zu Kopiengruppen für Archivierungsdateien abzufragen, geben Sie den Befehl **QUERY COPYGROUP** *Domänenname Name_der_Maßnahmengruppe Name_der_Verwaltungsklasse* **TYPE=ARCHIVE F=D** aus.
3. Geben Sie den Befehl **QUERY STGPOOL** *Speicherpoolname* aus; dabei ist *Speicherpoolname* das Ziel, das in den vorherigen Abfragen **QUERY COPYGROUP** zurückgemeldet wurde.
4. Geben Sie den Befehl **QUERY DEVCLASS** *Name_der_Einheitenklasse* für die Einheitenklasse aus, die vom Zielspeicherpool verwendet wird.
5. Geben Sie den Befehl **QUERY LIBRARY** *Speicherarchivname* für das Speicherarchiv aus, das für die vom Zielspeicherpool verwendete Einheitenklasse zurückgemeldet wurde.
6. Geben Sie den Befehl **QUERY DRIVE** *Speicherarchivname* **F=D** für das Speicherarchiv aus, das für die vom Zielspeicherpool verwendete Einheitenklasse angegeben wurde. Wenn für dieses Speicherarchiv keine Laufwerke definiert sind, überprüfen Sie die Speicherarchiv- und Laufwerkkonfiguration für diesen Server und definieren Sie die erforderlichen Laufwerke, indem Sie den Befehl **DEFINE DRIVE** ausgeben. Wenn für ein oder mehrere Laufwerke „ONLINE=No" zurückgemeldet wird, stellen Sie fest, warum das Laufwerk offline ist, und versetzen Sie es, falls möglich, in den Onlinestatus, indem Sie es mit dem Befehl **UPDATE DRIVE** *Speicherarchivname Laufwerkname* **ONLINE=YES** aktualisieren.
7. Geben Sie den Befehl **QUERY SERVER** aus, um den Namen des Speicheragenten zu bestimmen, der für diesen Server definiert ist.
8. Geben Sie den Befehl **QUERY PATH** *Name_des_Speicheragenten* aus; dabei ist *Name_des_Speicheragenten* der Name des für diesen Server definierten Speicheragenten, der für den Befehl **QUERY SERVER** zurückgemeldet wurde. Überprüfen Sie diese Ausgabe und stellen Sie sicher, dass ein oder mehrere Pfade für Laufwerke definiert sind, die für die vom Zielspeicherpool verwendeten Einheitenklassen definiert sind. Wenn für diesen Speicherpool keine Pfade definiert sind, definieren Sie die erforderlichen Pfade, indem Sie den Befehl **DEFINE PATH** ausgeben. Überprüfen Sie diese Ausgabe außerdem darauf, ob der Pfad online ist. Wenn Pfade zwar definiert, aber nicht online sind, versetzen Sie den

Pfad in den Onlinestatus, indem Sie ihn mit dem Befehl **UPDATE PATH** *Quellenname Zielname* **SRCTYPE=SERVER DESTTYPE=DRIVE ONLINE=YES** aktualisieren.

Problem eines Speicherpools beheben, der als LAN-unabhängig aktiviert ausgeschlossen wurde

Der Server schließt einen Speicherpool als LAN-unabhängig aktivierten Speicherpool aus, wenn er für gleichzeitiges Schreiben konfiguriert wurde.

In diesem Fall werden Daten vom Client direkt an einen Server gesendet, der keinen LAN-unabhängigen Speicherpool verwendet.

Geben Sie den Befehl **QUERY STGPOOL** *speicherpoolname* **F=D** für den Zielspeicherpool für diesen Client aus. Wenn der Speicherpool für gleichzeitiges Schreiben konfiguriert ist, verweist der Wert von „Kopienspeicherpool(s)" auf mindestens einen anderen Speicherpoolnamen und IBM Spectrum Protect interpretiert die Operation für gleichzeitiges Schreiben als höherrangig als die LAN-unabhängige Datenübertragung. Da Operationen für gleichzeitiges Schreiben als Operationen mit höherer Priorität betrachtet werden, wird dieser Speicherpool nicht als LAN-unabhängig aktiviert gemeldet, und die Daten werden daher vom Client direkt an den Server gesendet. Der Speicheragent unterstützt keine Operationen für gleichzeitiges Schreiben.

Datenübertragung in einer LAN-unabhängigen Umgebung sicherstellen

Der Speicheragent und der Client können beide direkte Übernahme durch den Server steuern, abhängig von der LAN-unabhängigen Konfiguration und dem Typ des aufgetretenen Fehlers.

Aufgrund dieser Übernahmefähigkeit ist es möglicherweise nicht ersichtlich, dass Daten über das LAN übertragen werden, wenn sie eigentlich LAN-unabhängig übertragen werden sollten. Es ist möglich, die LAN-unabhängige Umgebung so zu konfigurieren, dass die Datenübertragung ausschließlich auf LAN-unabhängige Übertragung beschränkt wird.

Um eine LAN-unabhängige Konfiguration zu testen, geben Sie den Befehl **UPDATE NODE** *Knotenname* **DATAWRITEPATH=LAN-FREE** für den Clientknoten aus, dessen LAN-unabhängige Konfiguration Sie testen wollen. Führen Sie anschließend eine Datenspeicherungsoperation durch, z. B. eine Sicherung oder Zurückschreibung. Wenn der Client und der Speicheragent versuchen, die Daten direkt über das LAN an den Server zu senden, wird folgende Fehlernachricht empfangen:

```
ANR0416W Sitzung Sitzungsnummer für Knoten Knotenname nicht zulässig für
Operation mit Datenübertragungspfad Pfad.
```

Die angezeigte *Operation* ist entweder READ oder WRITE, je nach ausgeführter Operation. Der Pfad wird als LAN-unabhängig angezeigt.

Wird diese Nachricht empfangen, wenn eine LAN-unabhängige Operation ausgeführt werden soll, prüfen und bestätigen Sie die Einstellungen für die LAN-unabhängige Operation. Wenn Daten nicht LAN-unabhängig gesendet werden, obwohl der Client für die LAN-unabhängige Übertragung konfiguriert ist, handelt es sich im Allgemeinen bei dem Speicherpoolziel für die Maßnahme, die diesem Knoten zugeordnet ist, nicht um einen LAN-unabhängig aktivierten Speicherpool oder die Pfade sind nicht ordnungsgemäß definiert.

Kapitel 7. Trace zur Behebung von Problemen verwenden

IBM Spectrum Protect kann gelegentlich Probleme feststellen, die Sie mithilfe von Trace beheben können.

Erweiterten Trace für das Operations Center starten

AIX Linux Windows

Das Operations Center-Protokoll enthält standardmäßig Daten aus einem Basistrace für Operations Center-Ereignisse. Der IBM Software Support fordert Sie möglicherweise auf, einen erweiterten Trace durchzuführen.

Informationen zu diesem Vorgang

Führen Sie eine der folgenden Prozeduren aus, um einen erweiterten Trace für das Operations Center durchzuführen:

Zugehörige Konzepte:

„Übersicht über Protokolldateien" auf Seite 107

Zugehörige Tasks:

„Operations Center-Protokoll im Operations Center anzeigen" auf Seite 108

Trace für Operations Center durchführen, indem Protokollierungsfunktionen innerhalb des Operations Center aktiviert werden

AIX Linux Windows

Im Operations Center können Sie Protokollierungsfunktionen aktivieren und einen erweiterten Trace starten, der dem Operations Center-Protokoll Fehlerbehebungsdaten hinzufügt.

Informationen zu diesem Vorgang

Mit der nachfolgend beschriebenen Vorgehensweise können Sie Gruppen von Protokollierungsfunktionen aktivieren und einen erweiterten Trace starten.

Achtung: Stellen Sie sicher, dass die Gruppen nach dem Trace wieder inaktiviert werden. Andernfalls kann die Leistung des Operations Center beeinträchtigt werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Trace für das Operations Center durchzuführen:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Fragezeichensymbol und wählen Sie **Informationen zum Operations Center** aus.
2. Klicken Sie auf **Installationsdetails**.
3. Klicken Sie auf die Registerkarte **Protokollierungsgruppe**.

4. Wählen Sie in der Liste mit den Protokollierungsgruppen nur die Zeilen aus, die der IBM Software Support von Ihnen anfordert, und klicken Sie auf **Aktivieren**.
5. Bestätigen Sie, dass Sie die Protokollierungsgruppen aktivieren möchten, und klicken Sie auf **Schließen**.
6. Reproduzieren Sie das Problem, das Sie beheben möchten. Für das Operations Center wird automatisch ein Trace durchgeführt und es wird eine neue Version des Operations Center-Protokolls erstellt.
7. Kehren Sie zur Liste mit den Protokollierungsgruppen zurück, indem Sie Schritt 1 auf Seite 121 bis Schritt 3 auf Seite 121 wiederholen.
8. Wählen Sie alle aktivierten Zeilen aus und klicken Sie auf **Inaktivieren**.
9. Bestätigen Sie, dass Sie die Protokollierungsgruppen inaktivieren möchten, und klicken Sie auf **Schließen**.

Nächste Schritte

Informationen zur Speicherposition und zu den Namen der Operations Center-Protokolldateien finden Sie in „Übersicht über Protokolldateien" auf Seite 107.

Zugehörige Tasks:

„Operations Center-Protokoll im Operations Center anzeigen" auf Seite 108

„Trace für Operations Center durchführen, indem Funktionen in der Konfigurationsdatei für die Protokollierung aktiviert werden"

Trace für Operations Center durchführen, indem Funktionen in der Konfigurationsdatei für die Protokollierung aktiviert werden

AIX Linux Windows

Wenn das Problem, für das Sie eine Fehlerbehebung durchführen, das Öffnen des Operations Center verhindert, können Sie die Konfigurationsdatei für die Protokollierung öffnen und ändern und anschließend einen erweiterten Trace starten, der dem Operations Center-Protokoll Daten hinzufügt.

Informationen zu diesem Vorgang

Mit der nachfolgend beschriebenen Vorgehensweise können Sie Gruppen von Protokollierungsfunktionen aktivieren und einen erweiterten Trace starten.

Achtung: Stellen Sie sicher, dass die Gruppen nach dem Trace wieder inaktiviert werden. Andernfalls kann die Leistung des Operations Center beeinträchtigt werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Trace für das Operations Center durchzuführen:

1. Stoppen Sie den Web-Server für das Operations Center.
2. Wechseln Sie in das folgende Verzeichnis:

   AIX Linux *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer

   Windows *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

Dabei steht *Installationsverzeichnis* für das Verzeichnis, in dem IBM Spectrum Protect installiert ist.

3. Speichern Sie eine Kopie der Protokollierungskonfigurationsdatei `OpsCntrLog.config` zur späteren Verwendung an einer anderen Position.
4. Öffnen Sie die ursprüngliche Datei `OpsCntrLog.config` in einem Texteditor.
5. Aktivieren Sie im Texteditor nur die Protokollierungsgruppen, deren Aktivierung der IBM Software Support bei Ihnen angefordert hat, indem Sie das Wort `OFF` für jede relevante Gruppe durch das Wort `ON` ersetzen.
6. Speichern und schließen Sie die Datei.
7. Starten Sie den Web-Server für das Operations Center.
8. Reproduzieren Sie das Problem, das Sie beheben möchten. Für das Operations Center wird automatisch ein Trace durchgeführt und es wird eine neue Version des Operations Center-Protokolls erstellt.
9. Stoppen Sie den Web-Server für das Operations Center.
10. Wechseln Sie erneut in das Verzeichnis `guiServer`.
11. Inaktivieren Sie die Protokollierungsgruppen, indem Sie die bearbeitete Datei `OpsCntrLog.config` durch die zuvor gespeicherte Kopie ersetzen.
12. Starten Sie den Web-Server für das Operations Center.

Nächste Schritte

Informationen zur Speicherposition und zu den Namen der Operations Center-Protokolldateien finden Sie in „Übersicht über Protokolldateien" auf Seite 107.

Zugehörige Tasks:

„Trace für Operations Center durchführen, indem Protokollierungsfunktionen innerhalb des Operations Center aktiviert werden" auf Seite 121

Trace für den Server oder Speicheragenten aktivieren

Sie können Tracebefehle von folgenden Stellen ausgeben: der Serverkonsole, der Konsole des Speicheragenten, dem Verwaltungsclient, der entweder mit dem Server oder dem Speicheragenten verbunden ist, der Serveroptionsdatei (`dsmserv.opt`) oder der Optionsdatei des Speicheragenten (`dsmsta.opt`).

Vorbereitende Schritte

Tracebefehle gelten für den Server oder Speicheragenten, an den der Befehl übergeben wurde. Tracebefehle in den Optionsdateien dienen zur Durchführung eines Trace für die Anwendungen während des Starts und der Initialisierung oder zur Bereitstellung einer Standardgruppe von Traceklassen. Eine Traceklasse, die Traceklasse **ADDMSG**, wird standardmäßig immer aktiviert, unabhängig davon, ob sie in der Optionsdatei angegeben ist oder nicht. Der Trace wird am besten in eine Datei ausgegeben. Normalerweise wird bei der Ausführung der Tracefunktion für den Server oder den Speicheragenten ein großes Ausgabevolumen generiert.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um Traceklassen für den Server oder den Speicheragenten zu aktivieren:

Vorgehensweise

1. Bestimmen Sie die Traceklassen, die aktiviert werden sollen. Damit Tracenachrichten für eine bestimmte Traceklasse ausgegeben werden, muss diese Trace-

klasse entweder vor dem Start des Trace aktiviert werden oder nachdem die Ausführung des Trace bereits begonnen hat.

2. Geben Sie den Befehl **TRACE ENABLE** *Name_der_Traceklasse* aus, um eine oder mehrere Traceklassen zu aktivieren. Beachten Sie, dass es sich bei *Name_der_Traceklasse* um eine Liste mit durch Leerzeichen getrennten Traceklassen handeln kann. Beispielsweise könnte dieser Befehl als **TRACE ENABLE TM SESSION** eingegeben werden. Der Befehl **TRACE ENABLE** ist kumulativ, sodass weitere Traceklassen aktiviert werden können, indem der Befehl **TRACE ENABLE** mehrmals ausgegeben wird. Soll beispielsweise die Traceklasse PVR zusätzlich zu den bereits aktivierten Traceklassen hinzugefügt werden, geben Sie den Befehl **TRACE ENABLE PVR** aus. Um die Ausgabe von Tracenachrichten für eine bestimmte Traceklasse zu stoppen, muss diese Traceklasse entweder vor dem Start des Trace inaktiviert werden oder nachdem die Ausführung des Trace bereits begonnen hat.
3. Geben Sie den Befehl **TRACE DISABLE**<*Name_der_Traceklasse*> aus, um eine oder mehrere Traceklassen zu inaktivieren. Beachten Sie, dass es sich bei *Name_der_Traceklasse* um eine Liste mit durch Leerzeichen getrennten Traceklassen handeln kann. Beispielsweise könnte dieser Befehl als **TRACE DISABLE TM SESSION** eingegeben werden. Weitere Traceklassen können ebenfalls durch Ausgabe des Befehls **TRACE DISABLE** inaktiviert werden. Soll beispielsweise die Traceklasse PVR zusätzlich zu den bereits inaktivierten Traceklassen entfernt werden, geben Sie den Befehl **TRACE DISABLE PVR** aus. Wird der Befehl **TRACE DISABLE** ohne Angabe von Traceklassen ausgegeben, werden alle derzeit aktivierten Traceklassen inaktiviert.
4. Die Tracenachrichten können an die Konsole oder in eine Datei geschrieben werden. Führen Sie die folgenden Tasks aus, um die Tracefunktion zu starten:
   - Um die Tracenachrichten an die Konsole zu schreiben, geben Sie den Befehl **TRACE BEGIN** aus.
   - Um die Tracenachrichten in eine Datei ohne Größenbegrenzung zu schreiben, geben Sie den Befehl **TRACE BEGIN** *Dateiname* aus.
   - Um die Tracenachrichten in eine Datei mit Größenbegrenzung zu schreiben, geben Sie den Befehl **TRACE BEGIN** *Dateiname* **MAXSIZE=** *maximale Größe in Megabyte* aus.

   Anmerkung: Der *Dateiname* kann ein vollständig qualifizierter Pfad wie `/opt/tmp` sein oder `c:\temp`. Wenn kein vollständiger Pfad angegeben wird, wird die Tracedatei in demselben Verzeichnis wie die aktive ausführbare Datei gespeichert.
5. Führen Sie die Operation aus, die den Fehler verursacht.
6. Geben Sie den Befehl **TRACE END** aus, um die Ausgabe von Tracenachrichten zu stoppen. Wenn die Tracenachrichten in eine Datei ausgegeben werden, werden bei Beendigung des Trace alle verbleibenden Tracenachrichten in die Datei geschrieben und die Datei geschlossen.

Nächste Schritte

Es ist möglich, die Tracefunktion zu aktivieren und mithilfe der Optionsdatei des Servers oder des Speicheragenten zu starten. Die Befehle und die Syntax sind für die Optionsdatei des Servers und die Optionsdatei des Speicheragenten identisch; im Allgemeinen dienen sie zur Durchführung eines Trace während des Starts und der Initialisierung des Servers. Würden beispielsweise die folgenden Zeilen der Serveroptionsdatei hinzugefügt, würde die Tracefunktion für die Traceklassen DB, TM und LOG gestartet und die Tracenachrichten würden in die Datei `MYTRACE.OUT` geschrieben.

```
TRACE ENABLE DB TM LOG
TRACE BEGIN MYTRACE.OUT BUFSIZE=4096
```

Hinweis: Wenn Sie einen Trace wegen eines Serverabsturzes durchführen, dürfen Sie nicht den Parameter **BUFSIZE** definieren.

Zugehörige Verweise:

„Traceklassen für einen Server oder Speicheragenten" auf Seite 126

Stack-Trace für Nachrichten für den Server oder Speicheragenten aktivieren

Ein Stack-Trace zeigt Informationen zu einer Anwendung an, die der IBM Software Support verwenden kann, um Ihre Probleme schneller zu diagnostizieren.

Anmerkung: Je nach Häufigkeit des Fehlers kann ein Stack-Trace die Aktivitätenprotokolldatei mit so vielen Informationen füllen, dass bei dem Versuch, die Aktivitätenprotokolldatei anzuzeigen, Probleme auftreten. Es kann sinnvoll sein, den Stack-Trace nach seinem Abschluss zu inaktivieren.

Für den IBM Software Support ist es möglicherweise hilfreich, den Stack-Trace für bestimmte Nachrichten, die vom Server oder Speicheragenten ausgegeben werden, zu aktivieren. Die Typen von Nachrichten, für die ein Stack-Trace aktiviert werden kann, sind die Serverkonsole, die Konsole des Speicheragenten und der Verwaltungsclient, der entweder mit dem Server oder dem Speicheragenten verbunden ist.

Um einen Stack-Trace abzurufen, wenn eine bestimmte Nachricht vom Server oder Speicheragenten ausgegeben wird, aktivieren Sie die Nachricht für den Stack-Trace. Geben Sie den Befehl **MSGSTACKTRACE ENABLE** <*Nachrichtennummer*> aus, um eine oder mehrere Nachrichten für den Stack-Trace zu aktivieren.

Hinweis: <*Nachrichtennummer*> kann eine durch Leerzeichen getrennte Liste von Nachrichtennummern sein.

Dieser Befehl kann als **MS ENABLE 2017** eingegeben werden. Der Befehl **MSGSTACKTRACE ENABLE** ist kumulativ, sodass weitere Nachrichten aktiviert werden können, indem der Befehl **MSGSTACKTRACE ENABLE** mehrmals ausgegeben wird. Soll beispielsweise die Nachricht 985 zusätzlich zu den bereits aktivierten Nachrichten hinzugefügt werden, geben Sie den Befehl **MS ENABLE 985** aus. Beachten Sie, dass nur die Nummer der Nachricht im Befehl **MSGSTACKTRACE** angegeben werden darf. Um das Abrufen des Stack-Trace für Nachrichten zu stoppen, die vom Server oder Speicheragenten ausgegeben werden, muss der Stack-Trace für diese Nachrichten inaktiviert werden. Geben Sie den Befehl **MSGSTACKTRACE DISABLE** <*Nachrichtennummer*> aus, um eine oder mehrere Nachrichten zu inaktivieren.

<*Nachrichtennummer*> kann eine durch Leerzeichen getrennte Liste von Nachrichtennummern sein. Beispielsweise kann dieser Befehl als **MSGSTACKTRACE DISABLE 2017 985** eingegeben werden. Zusätzliche Nachrichten können ebenfalls durch Ausgabe des Befehls **MS DISABLE** inaktiviert werden. Soll beispielsweise die Nachrichtennummer 7837 zusätzlich zu den bereits inaktivierten Nachrichten entfernt werden, geben Sie den Befehl **MSGSTACKTRACE DISABLE 7837** aus.

Die folgenden Nachrichten sind standardmäßig für den Stack-Trace aktiviert:

```
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
```

Traceklassen für einen Server oder Speicheragenten

Der Server und der Speicheragent stellen zusammengefasste Traceklassen bereit. Diese Traceklassen sind ein Direktaufruf für die Verwendung vieler verwandter Traceklassen. Dabei wird der Name der zusammengefassten Traceklasse im Befehl **TRACE ENABLE** angegeben.

Die in Tabelle 10 aufgelisteten Traceklassen sind die Traceklassen, die am häufigsten angefordert oder für die Diagnose von Problemen verwendet werden. Diese Tabelle enthält nicht alle Traceklassen, die verfügbar sind. Der Name der Traceklasse wird mit den Befehlen **TRACE ENABLE** und **TRACE DISABLE** verwendet.

Tabelle 10. Traceklassen für den Server oder Speicheragenten

Traceklassen	Beschreibung	Verwendung
ADDMSG	Gibt Konsolennachrichten wie z. B. ANR- und ANE-Nachrichten an die Tracedatei aus.	Diese Traceklasse ist wichtig, um Servernachrichten und Tracenachrichten zu korrelieren und die Zeit aufzuzeichnen, zu der die Nachrichten ausgegeben wurden.
ADMCMD	Traces, die sich auf die Befehlsverarbeitung beziehen.	Verwenden Sie diese Traceklasse, um den Befehlsinterpreter zu testen, einschließlich der Verarbeitung der Befehle **PARALLEL** und **SERIAL**.
AF	Diese Traceklasse zeigt Informationen zu Benutzerdaten an, die auf Einheiten für sequenzielle Datenträger gespeichert werden. AF ist eine zusammengefasste Traceklasse, die AFCREATE, AFMOVE, AFLOCK, AFTXN und AFCOPY verwendet. Geben Sie **TRACE DISABLE AFLOCK** aus, es sei denn, die Informationen über Sperren werden explizit angefordert oder benötigt.	Verwenden Sie diese Traceklasse, um Probleme beim Lesen von Benutzerdateien von sequenziellen Datenträgern oder beim Schreiben von Benutzerdateien auf sequenzielle Datenträger zu diagnostizieren.
AFCREATE	Diese Traceklasse zeigt Informationen zum Speichern von Benutzerdaten auf sequenziellen Datenträgern an.	Verwenden Sie diese Traceklasse, um Probleme beim Schreiben von Benutzerdaten auf sequenzielle Datenträger zu diagnostizieren.
AFMOVE	Diese Traceklasse zeigt Operationen an, mit denen Benutzerdaten auf sequenziellen Datenträgern versetzt werden. Versetzungsoperationen werden von den Serverprozessen MIGRATION, RECLAMATION, MOVE DATA und MOVE NODEDATA ausgeführt.	Verwenden Sie diese Traceklasse, um Probleme mit den Serverprozessen für die Datenversetzung zu diagnostizieren.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
AS	Diese Traceklasse zeigt Informationen zur Datenträgerauswahl und -zuordnung, zur Koordination von Laufwerken (Mountpunkten) und zur Verwaltung der Datenplatzierung auf Datenträgern an. Diese zusammengefasste Traceklasse verwendet ASALLOC, ASRTRV, ASDEALLOC, ASMOUNT, ASVOL, ASTXN und ASSD. Die typische Methode ist die Ausgabe von TRACE DISABLE ASTXN, es sei denn, die Informationen über Sperren werden explizit angefordert oder benötigt.	Verwenden Sie diese Traceklasse, um viele verschiedene Probleme mit Datenträgern, Mountpunkten oder Datenlese- und -schreiboperationen zu diagnostizieren.
ASALLOC	Diese Traceklasse zeigt Informationen zum Reservieren und Zuordnen von Speicherbereich auf sequenziellen Datenträgern zum Speichern von Daten an. Dieser Speicherbereich dient zum Speichern von Daten für eine Clientsitzung oder für Serverdatenversetzungsoperationen, wie z. B. MIGRATION, RECLAMATION, MOVE DATA oder MOVE NODEDATA.	Diagnostizieren Sie Probleme, wenn der Server oder Speicheragent zurückmeldet, dass kein Speicherbereich verfügbar ist, aber Speicherbereich in der Speicherhierarchie verfügbar sein müsste.
ASDEALLOC	Diese Traceklasse zeigt Informationen zur Freigabe und Aufhebung der Zuordnung von Speicherbereich auf sequenziellen Datenträgern zum Speichern von Daten an. Typische Freigabeoperationen auf dem Server sind **EXPIRATION**, **MIGRATION**, **RECLAMATION**, **MOVE DATA**, **MOVE NODEDATA**, **AUDIT VOLUME**, **DELETE VOLUME** und **DELETE FILESPACE**.	Verwenden Sie diese Traceklasse, um Probleme während des Löschens von Daten zu diagnostizieren.
ASMOUNT	Diese Traceklasse zeigt Informationen zur Laufwerkauswahl und -zuordnung (Mountpunkt) auf Einheiten für sequenzielle Datenträger an.	Diagnostizieren Sie Situationen, in denen Sitzungen oder Prozesse auf Mountpunkte warten, oder Fälle, in denen eine Operation fehlschlägt, weil kein Mountpunkt verfügbar ist. Auch nützlich in Fällen, in denen ein Mountpunkt zurückgestellt wird.
ASRTRV	Diese Traceklasse zeigt Informationen zum Lesen von Daten von sequenziellen Datenträgern an.	Verwenden Sie diese Traceklasse, um Probleme mit Daten zu diagnostizieren, wie z. B. **RESTORE** oder **RETRIEVE** (durch den Client) oder **MIGRATION**, **RECLAMATION**, **STORAGE POOL BACKUP**, **AUDIT VOLUME**, **GENERATE BACKUPSET**, **EXPORT**, **MOVE DATA** oder **MOVE NODEDATA** (durch den Server).

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
ASTXN	Diese Traceklasse zeigt Informationen zu Transaktionen an, die zur Durchführung von Datenbankaktualisierungen für Informationen zu sequenziellen Datenträgern, Speicherpools, Einheitenklassen und anderen Attributen verwendet werden.	Verwenden Sie diese Traceklasse, um Stopps, Datenbankoperationen, Fehler, die für Operationen mit sequenziellen Datenträgern zurückgemeldet werden, oder allgemeine Datenspeicherprobleme zu diagnostizieren.
ASVOL	Diese Traceklasse zeigt Informationen zur Datenträgerauswahl und -zuordnung für sequenzielle Datenträger an.	Verwenden Sie diese Traceklasse, um Situationen zu diagnostizieren, in denen Sitzungen oder Prozesse auf Datenträger warten, oder Fälle zu diagnostizieren, in denen eine Operation fehlschlägt, weil kein Datenträger verfügbar ist. Auch nützlich in Fällen, in denen der Datenträgerzugriff zurückgestellt wird.
ASSD	Diese Traceklasse zeigt Informationen zu sequenziellen Datenstromoperationen an. Diese Operationen verwenden die Einheitenklassen für sequenzielle Datenträger, Datenträger oder Mountpunkte, speichern aber keine Daten in der Speicherhierarchie. BACKUP DB, EXPORT/IMPORT und GENERATE BACKUPSET sind Serverprozesse, die sequenzielle Datenstromoperationen ausführen.	Verwenden Sie diese Traceklasse, um Serverprozesse zu diagnostizieren, die sequenzielle Datenstromoperationen ausführen.
BF	Informationen zu Benutzerdaten (Dateien), die in der Speicherhierarchie gespeichert sind. Diese zusammengefasste Traceklasse verwendet **BFCREATE**, **BFRTRV**, **BFSALVAGE**, **BFLOCK**, **BFAGGR**, **BFREMOTE**, **BFSAGGR** und **BFTRG**.	Verwenden Sie diese Traceklasse, um allgemeine Probleme beim Lesen oder Schreiben von Daten für Clientoperationen und Serverprozesse zu diagnostizieren.
BFAGGR	Diese Traceklasse zeigt Informationen zur Zusammenfassung von Benutzerdaten durch den Server an. Der Server fasst viele kleinere Benutzerdateien in einer größeren Datei in der Speicherhierarchie zusammen, um die Leistung für Operationen zum Versetzen von Daten, wie z. B. **MIGRATION**, **MOVE DATA** und **MOVE NODEDATA**, zu optimieren.	Verwenden Sie diese Traceklasse, um allgemeine Probleme beim Lesen oder Schreiben von Daten für Clientoperationen und Serverprozesse zu diagnostizieren.
BFCREATE	Diese Traceklasse zeigt Informationen zu Clientoperationen an, die Daten in der Speicherhierarchie speichern. Normalerweise sind diese Clientoperationen **BACKUP**, **ARCHIVE** oder **SPACE MANAGE**-Operationen durch den Client.	Verwenden Sie diese Traceklasse, um Fehler oder andere Probleme zu diagnostizieren, während ein Client Daten speichert.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
BFREMOTE	Erstellt einen Trace für die erste Stufe von NDMP-Sicherungs- und -Zurückschreibungsprozessen (NDMP = Network Data Management Protocol).	Diese Traceklasse wird verwendet, um NDMP-bezogene Sicherungs- oder Zurückschreibungsoperationen zu identifizieren. Diese Traceklassen sind für die Funktionen bestimmt, die das NDMP-Protokoll implementieren. Die Traceklasse SPID stellt eine ausführlichere Traceerstellung bereit, einschließlich einer Traceerstellung für alle NDMP-Protokolldateisätze, die vom NDMP-Dateiserver gesendet werden.
BFRTRV	Diese Traceklasse zeigt Informationen zu Clientoperationen an, die Daten aus der Speicherhierarchie lesen.	Verwenden Sie diese Traceklasse, um Fehler oder andere Probleme zu diagnostizieren, während ein Client Daten liest.
BFSAGGR	Diese Traceklasse zeigt Informationen zum Speichern, Abrufen und Versetzen von Superaggregaten an. Ein Objekt mit einer Größe von mehr als 10 GB wird als Superaggregat gespeichert.	Verwenden Sie diese Traceklasse für die Diagnose von Problemen beim Speichern oder Abrufen von Objekten, die größer als 10 GB sind.
BITVECTOR	Diagnostiziert Situationen, in denen der Server Probleme mit Plattenspeicherpools zurückmeldet.	Verwenden Sie diese Traceklasse, um Informationen zum Reservieren und Zuordnen von Speicherbereich auf Datenträgern in Plattenspeicherpools anzuzeigen.
BKSET/OBJSET	Traceklasse für Sicherungsgruppenfunktionen. Die Traceklassen BKSET und OBJSET sind synonym.	Verwenden Sie diese Traceklasse, um Fehler im Befehl GENERATE BACKUPSET oder während einer Clientzurückschreibungsoperation aus einer Sicherungsgruppe zu beheben.
BLKDISK	Traceklasse zum Anzeigen der Platten-E/A-Aktivität für Speicherpool-, Datenbank- und Protokolldatenträger.	Verwenden Sie diese Traceklasse zum Anzeigen der Platten-E/A-Aktivität, um Leistungsprobleme und Platten-E/A-Fehler zu diagnostizieren.
BRNODE	Traceklasse für die Befehle **BACKUP** und **RESTORE NODE**, die während der Ausführung von NDMP-Operationen verwendet werden.	Verwenden Sie diese Traceklasse, um Fehler in den Befehlen **BACKUP** und **RESTORE NODE** zu beheben.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
COLLOCATE	Diese Traceklasse zeigt Informationen zur Kollokationsverarbeitung für Speicherpools an. Die Traceklasse COLLOCATEDETAIL kann ebenfalls verwendet werden, um detaillierte Informationen zur Kollokationsverarbeitung abzurufen. Ein Beispiel sind Informationen zu den Dateien, die für eine Kollokationsgruppe verarbeitet werden. Dateien, die für eine Kollokationsgruppe verarbeitet werden, können viele Ausgabetraceanweisungen zur Folge haben.	Verwenden Sie diese Traceklasse, um Probleme mit der Kollokationsverarbeitung zu diagnostizieren.
CRC	Diese Traceklasse zeigt Informationen zum Generieren und Steuern von zyklischen Blockprüfungen (Cyclic Redundancy Checks = CRCs) auf dem Server oder Speicheragenten an. CRC ist eine zusammengefasste Traceklasse, die **CRCDATA**, **CRCPROTO** und **CRCVAL** verwendet.	Verwenden Sie diese Traceklasse, um Probleme mit fehlerhaften Daten zu diagnostizieren, wobei die CRC-Verarbeitung keine fehlerhaften Daten zurückgemeldet hat.
CRCDATA	Diese Traceklasse zeigt Informationen zum Generieren und Steuern von CRCs für Daten an, die in Speicherpools mit `CRCDATA=YES` gespeichert sind.	Verwenden Sie diese Traceklasse, um Probleme mit fehlerhaften Daten zu diagnostizieren, wobei die CRC-Verarbeitung keine fehlerhaften Daten zurückgemeldet hat.
CRCPROTO	Diese Traceklasse zeigt Informationen zum Generieren und Steuern von CRCs für Daten an, die zwischen dem Client und dem Server oder Speicheragenten ausgetauscht werden, wobei dieser Knoten mit `VALIDATEPROTOCOL=ALL` oder `VALIDATEPROTOCOL=DATAOnly` auf dem Server konfiguriert ist.	Verwenden Sie diese Traceklasse, um Probleme mit fehlerhaften Daten zu diagnostizieren, wobei die CRC-Verarbeitung keine fehlerhaften Daten zurückgemeldet hat.
CRCVAL	Diese Traceklasse zeigt Informationen zum Generieren und Vergleichen von CRC-Werten an.	Informationen, die CRC-Werte während der Verarbeitung anzeigen.
CRYPTO	Diese Traceklasse zeigt Informationen zu Advanced Encryption Standard-Operationen und zu einigen allgemeinen Verschlüsselungseinstellungen an.	Verwenden Sie diese Traceklasse, um Probleme einzugrenzen und zu identifizieren, die sich auf die Verschlüsselung beziehen.
DBCLI	Erstellt einen Trace für die allgemeine Gruppe von Interaktionen.	Verwenden Sie diese Traceklasse, um einen Trace für die allgemeine Gruppe von DB2-Interaktionen und die DB2-Befehlszeilenschnittstelle zu erstellen.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
DBCONN	Erstellt einen Trace für Verbindungsaktivitäten.	Verwenden Sie diese Traceklasse, um einen Trace für IBM Spectrum Protect-Verbindungen zu DB2-Verbindungen zu erstellen. Diese Traceklasse zeigt Informationen wie z. B. die Erstellung von Verbindungskennungen und die Zuordnung von Verbindungen zu Transaktionen an.
DBDBG	Erstellt einen Trace für Debug-Prozesse. Diese Traceklasse könnte zuerst verwendet werden, wenn ein Debug für eine Datenbank ausgeführt wird.	Verwenden Sie diese Traceklasse, um den Funktionseingang oder -ausgang, die Ausgangsrückkehrcodes und die Anweisungen anzuzeigen, die erstellt und ausgeführt werden.
DBITXN	Erstellt einen Trace für Aktivitäten, die sich auf Datenbanktransaktionen beziehen. Transaktionsbezogene Aktivitäten betreffen die Anforderung und Freigabe von Transaktionssperren, die dbTxnDesc-Zuordnung und -Freigabe sowie die Transaktionscommitverarbeitung der Funktionen für die Vorbereitungs- und Festschreibungsphase (Prepare und Commit).	Verwenden Sie diese Traceklasse, um einen Trace für transaktionsbezogene Aktivitäten für die Datenbankschnittstelle zu erstellen.
DBNETDB	Diese Traceklasse zeigt Informationen zu LAN-unabhängigen Operationen und zur Festlegung und Verwaltung von Informationen zwischen dem Server und dem Speicheragenten an.	Mithilfe dieser Traceklasse können Sie LAN-unabhängige Probleme diagnostizieren, wenn Server und Speicheragent ein unterschiedliches Release-Level aufweisen. Sie funktionieren besser, wenn sie dasselbe Release-Level aufweisen. Sie können mit dieser Traceklasse auch Probleme bei einem Speicheragenten diagnostizieren, der Konfigurationsinformationen vom Server abruft.
DBRC	Erstellt einen Trace für die Rückkehrcodes aus Funktionen in der Datenbankkomponente.	Verwenden Sie diese Traceklasse, um einen Trace für die Rückkehrcodes zu erstellen.
DEDUP	Erstellt einen Trace für den allgemeinen Logikpfad bei der Datendeduplizierungsverarbeitung. Enthält normalerweise keine Fehlerpfade.	Verwenden Sie DEDUP, um einen Trace für allgemeine Logikpfade bei der Datendeduplizierungsverarbeitung zu erstellen.
DEDUP1	Erstellt einen Trace für Fehlerpfade bei der Datendeduplizierungsverarbeitung.	Verwenden Sie DEDUP1, um einen Trace für Fehlerpfade bei der Datendeduplizierungsverarbeitung zu erstellen.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
DEDUP2	Erstellt einen Trace für den Pfad für Fingerabdrücke und digitale Signaturen.	Verwenden Sie DEDUP2, um einen Trace für Pfade für Fingerabdrücke und digitale Signaturen zu erstellen.
DELTA	Traceklasse für Funktionen für logische Gruppen. Die Traceklassen DELTA und GROUP sind synonym.	Verwenden Sie diese Traceklasse, um Fehler für logische Gruppen zu beheben. Hierbei kann es sich um Deltabasisgruppen (Subdateisicherung) oder Peergruppen (Windows SYSTEM OBJECT-Sicherung oder Imagesicherung) handeln. Die Gruppenverarbeitung ist für jede Operation wichtig, die auf Sicherungsobjekte verweist. Die Sicherungsobjekte können Clientsicherung und -zurückschreibung, Verfallsverarbeitung, Löschen (**DELETE FILESPACE**, **DELETE VOLUME**), Export/Import, Erstellung und Zurückschreibung von Sicherungsgruppen, Zurückschreibung ohne Abfrage, Datenbankprüfung und andere einschließen.
DF	Diese Traceklasse zeigt Informationen zu Benutzerdaten an, die auf Plattendatenträgern gespeichert werden. DF ist eine zusammengefasste Traceklasse, die **DFCREATE**, **DFRTRV**, **DFMOVE**, **DFLOCK**, **DFTXN** und **DFCOPY** aktiviert. Geben Sie den Befehl **TRACE DISABLE DFLOCK** aus, es sei denn, die Informationen über Sperren werden explizit angefordert oder benötigt.	Verwenden Sie diese Traceklasse, um Probleme beim Lesen oder Schreiben von Benutzerdateien auf Plattendatenträger zu diagnostizieren.
DFCREATE	Diese Traceklasse zeigt Informationen zum Speichern von Benutzerdaten auf Plattendatenträgern an.	Verwenden Sie diese Traceklasse, um Probleme beim Schreiben von Benutzerdaten auf Plattendatenträger zu diagnostizieren.
DFMOVE	Diese Traceklasse zeigt Operationen an, mit denen Benutzerdaten unter Verwendung von Plattendatenträgern versetzt werden. Versetzungsoperationen werden von den Serverprozessen MIGRATION, MOVE DATA und MOVE NODEDATA ausgeführt.	Verwenden Sie diese Traceklasse, um Probleme mit den Serverprozessen für die Datenversetzung zu diagnostizieren.
DFRTRV	Diese Traceklasse zeigt Informationen zum Lesen von Benutzerdaten von Plattendatenträgern an.	Verwenden Sie diese Traceklasse, um Probleme beim Lesen von Benutzerdaten von Plattendatenträgern zu diagnostizieren.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
DS	Diese Traceklasse zeigt Informationen zur Datenträgerauswahl, Bereichsreservierung, Zuordnung und Verwaltung der Datenplatzierung auf Plattendatenträgern an. DS ist eine zusammengefasste Traceklasse, die DSALLOC, DSRTRV, DSDEALLOC und DSVOL aktiviert. Geben Sie **TRACE DISABLE DSTXN** aus, es sei denn, die Informationen über Sperren werden explizit angefordert oder benötigt.	Verwenden Sie diese Traceklasse, um viele verschiedene Probleme bei Datenlese- und -schreiboperationen für Plattendatenträger zu diagnostizieren.
DSALLOC	Diese Traceklasse zeigt Informationen zum Reservieren und Zuordnen von Speicherbereich auf Plattendatenträgern zum Speichern von Daten an. Die Datenspeicherung kann für eine Clientsitzung oder für Serverdatenversetzungsoperationen, wie z. B. **MIGRATION**, **MOVE DATA** oder **MOVE NODEDATA**, erfolgen.	Diagnostizieren Sie Probleme, wenn der Server oder Speicheragent zurückmeldet, dass kein Speicherbereich verfügbar ist, aber Speicherbereich in der Speicherhierarchie verfügbar zu sein scheint.
DSDEALLOC	Diese Traceklasse zeigt Informationen zur Freigabe und Aufhebung der Zuordnung von Speicherbereich auf Plattendatenträgern an. Typische Freigabeoperationen auf dem Server sind **EXPIRATION**, **MIGRATION**, **MOVE DATA**, **MOVE NODEDATA**, **AUDIT VOLUME**, **DELETE VOLUME** und **DELETE FILESPACE**.	Verwenden Sie diese Traceklasse, um Probleme während des Löschens von Daten zu diagnostizieren.
DSRTRV	Diese Traceklasse zeigt Informationen zum Lesen von Daten von Plattendatenträgern an.	Verwenden Sie diese Traceklasse, um Probleme beim Lesen von Daten zu diagnostizieren, wie z. B. **RESTORE** oder **RETRIEVE** (durch den Client) oder **MIGRATION**, **STORAGE POOL BACKUP**, **AUDIT VOLUME**, **GENERATE BACKUPSET**, **EXPORT**, **MOVE DATA** oder **MOVE NODEDATA** (durch den Server).
DSVOL	Diese Traceklasse zeigt Informationen zur Datenträgerauswahl und -zuordnung für Plattendatenträger an.	Verwenden Sie diese Traceklasse, um Situationen zu diagnostizieren, in denen Sitzungen oder Prozesse auf Datenträger warten, oder Fälle zu diagnostizieren, in denen eine Operation fehlschlägt, weil kein Datenträger verfügbar ist.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
ICVOLHST	Traceklasse für Datenträgerprotokollfunktionen.	Verwenden Sie diese Traceklasse, um Fehler bei der Erstellung von Datenträgerprotokolleinträgen (z. B. während der Ausführung von **EXPORT**, **BACKUP DB** oder **GENERATE BACKUPSET**) oder beim Löschen von Datenträgerprotokolleinträgen (z. B. während der Ausführung von **DELETE VOLHISTORY**) zu beheben.
IMFS	Traceklasse für Dateibereichsfunktionen.	Verwenden Sie diese Traceklasse, um Fehler für Bestandsdateibereiche zu beheben (z. B. während der Ausführung von **DELETE FILESPACE**).
LANFREE	Diese Traceklasse zeigt allgemeine Informationen zu LAN-unabhängigen Operationen auf dem Server oder Speicheragenten an. Zeigt außerdem Fehlerinformationen zu LAN-unabhängigen Operationen an. LANFREE ist eine zusammengefasste Traceklasse, die LNFVERB, LNFMEM, LNFENTRY und LNFDATA aktiviert.	Beliebiger LAN-unabhängiger Fehler.
MMS	Diese Traceklasse zeigt Informationen zu Bandarchiven und zu dem Server oder dem Speicheragenten an, der diese Bandarchive verwendet. MMS ist eine zusammengefasste Traceklasse, die MMSBASE, MMSTXN, MMSLIB, MMSDRIVE, MMSOP, MMSMAN, MMSSCSI, MMSFLAG, MMSACSLS und MMSSHARE aktiviert. Schließen Sie die Traceklassen NA und PVR bei der Traceerstellung mit MMS ein.	Wird verwendet, um Probleme mit Bandarchiven und dem Datenträgerbestand im Archiv oder andere allgemeine Probleme mit dem Archiv zu diagnostizieren.
MONITOR	Diese Traceklasse zeigt Informationen zur Alertüberwachung an.	Verwenden Sie diese Traceklasse, um zu ermitteln, warum ein Alert möglicherweise nicht generiert wurde.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
NA	Diese Traceklasse zeigt Informationen zu Pfadangaben für den Server oder Speicheragenten an. Diese Informationen beziehen sich auf die Befehle **DEFINE PATH**, **UPDATE PATH**, **DELETE PATH** und **QUERY PATH**. Diese Traceklasse wird auch verwendet, um Probleme zu identifizieren, die sich auf Operationen mit NDMP-Dateiservern beziehen, beispielsweise bei den Befehlen **DEFINE DATAMOVER**, **UPDATE DATAMOVER**, **BACKUP NODE** und **RESTORE NODE**. Diese zusammengefasste Traceklasse verwendet NALOCK, NAPATH, NAMOVER, NADISK und NACONFIG. Die besten Ergebnisse werden möglicherweise erzielt, wenn Sie die Traceklassen MMS und PVR bei der Traceerstellung mit NA einschließen.	Verwenden Sie diese Traceklasse, um Probleme mit Pfaden zu Einheiten zu diagnostizieren.
PRODCONS	Treten bei der Zuteilung von Arbeit zu Batches Probleme auf, zeigt PRODCONS Informationen zu dem Problem und dazu an, ob sich das Problem auf das PC-Objekt oder auf die Replikation bezieht.	Verwenden Sie PRODCONS, um einen Trace für die interne Arbeitsweise der Producer/Consumer-Objekte zu erstellen, die auf dem Server verwendet werden.
PROXYNODE	Diese Traceklasse zeigt Informationen zu Proxyknotensitzungen und zu den Befehlen an, die sich auf Proxyknotenzuordnungen beziehen (GRANT, REVOKE, QUERY PROXYNODE).	Verwenden Sie diese Traceklasse, um Probleme mit Proxyknotensitzungen und verwandten Befehlen zu diagnostizieren. Die besten Ergebnisse werden möglicherweise erzielt, wenn Sie die Traceklasse SESSION bei der Analyse von Problemen bezüglich Proxyknotensitzungen einschließen.
PVR	Diese Traceklasse zeigt Informationen zu Einheiten für sequenzielle Datenträger und zur Verwendung dieser Einheiten durch den Server oder Speicheragenten an. PVR ist eine zusammengefasste Traceklasse, die PVRVOL, PVRCLASS und PVRMP aktiviert. Die Traceklasse PVR enthält alle Traceklassen in der zusammengefassten Traceklasse PVRIO und die Traceklasse PVRNOIO.	Verwenden Sie diese Traceklasse, um Probleme mit Bandlaufwerken, Fehler beim Lesen oder Schreiben von Banddatenträgern oder andere Probleme zu diagnostizieren, die sich auf Banddatenträger beziehen.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
PVRIO	Diese Traceklasse zeigt einen Trace zu Lese-, Schreib- oder POS-Operationen für Einheiten für sequenzielle Datenträger und zur Verwendung dieser Einheiten durch den Server oder Speicheragenten an.	Verwenden Sie diese Traceklasse, um Probleme mit Bandlaufwerken und Fehler beim Lesen oder Schreiben von Banddatenträgern zu diagnostizieren.
PVRNOIO	Diese Traceklasse zeigt PVRVOL-, PVRCLASS- und PVRMP-Informationen an.	Verwenden Sie diese Traceklasse, um Probleme mit Bandlaufwerkmounts oder andere Probleme zu diagnostizieren, die sich auf Banddatenträger beziehen.
REPL	REPL ist eine zusammengefasste Traceklasse, die REPLBATCH, REPLCMD, REPLFS, REPLINV, REPLPROC, REPLSTATS und REPLSESS aktiviert.	Verwenden Sie diese Traceklasse, um Probleme mit der Replikation zu diagnostizieren.
REPLBATCH	Diese Traceklasse zeigt einen Trace für die Stapelverarbeitung an, bei der einzelne Dateien vom Quellenserver zum Zielserver gesendet werden.	Verwenden Sie diese Traceklasse, um Replikationsprobleme mit der Stapelverarbeitung zu diagnostizieren.
REPLCMD	Diese Traceklasse zeigt einen Trace für das Befehlsparsing und die Auflösung von Dateibereichsreplikationsregeln.	Verwenden Sie diese Traceklasse, um Replikationsprobleme mit dem Befehlsparsing und der Auflösung von Dateibereichsreplikationsregeln zu diagnostizieren.
REPLFS	Diese Traceklasse zeigt einen Trace zur Iteration von Dateibereichen an, anhand dessen entschieden werden kann, welche Objekte repliziert, aktualisiert oder gelöscht werden müssen.	Verwenden Sie diese Traceklasse für die Diagnose von Replikationsproblemen mit der Iteration von Dateibereichen, um zu entscheiden, welche Objekte repliziert, aktualisiert oder gelöscht werden müssen.
REPLINV	Diese Traceklasse zeigt einen Trace für die Bestandsaktualisierungen (IM-Tabellen) als Teil der Replikation an.	Verwenden Sie diese Traceklasse, um Replikationsprobleme mit Bestandsaktualisierungen zu diagnostizieren.
REPLPROC	Diese Traceklasse zeigt einen Trace für den gesamten Replikationsprozess an. Diese Traceklasse ist der Hauptthread und Dispatcher.	Verwenden Sie diese Traceklasse, um Replikationsprobleme mit dem Replikationsprozess zu diagnostizieren.
REPLSESS	Diese Traceklasse zeigt einen Trace zum Aufbau von Sitzungen für die Replikation an, einschließlich der Sitzungsverwaltung auf dem Quellen- und Zielserver.	Verwenden Sie diese Traceklasse, um Replikationsprobleme mit dem Aufbau von Sitzungen zu diagnostizieren.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
REPLSTATS	Diese Traceklasse zeigt einen Trace zur Aktualisierung der Statistik während der Replikation an. Schließt auch die Einfügung oder Aktualisierung von Protokollsätzen in der Replikationsprotokolltabelle ein.	Verwenden Sie diese Traceklasse, um Replikationsprobleme mit Statistikaktualisierungen zu diagnostizieren.
RETPROT	Traceklasse für die Funktionen zum Aufbewahrungsschutz für Archivierung.	Verwenden Sie diese Traceklasse, um Fehler bei der Verwendung der Parameter **RETINIT** und **RETMIN** in der Archivierungskopiengruppe zu beheben. Sie können diese Traceklasse auch für Probleme verwenden, die durch die Verwendung des Verbs 'VB_SignalObject' (wird nur von der Client-API unterstützt) verursacht werden, um das Ereignis eines Objekts zu signalisieren oder ein Objekt zu sperren oder freizugeben. Darüber hinaus kann diese Traceklasse für Probleme verwendet werden, die während der Verfallsverarbeitung oder beim Löschen von Objekten, die durch die Aufbewahrungsdauer geschützt sind, auftreten.
ROWMGR	Erstellt einen Trace zu Aktivitäten für zeilenbasierte Operationen. Zeilenbasierte Operationen sind die folgenden Operationen: • Abbrev • Delete • Fetch • FetchNext • FetchPrev • Insert • SearchBounds • Update	Verwenden Sie diese Traceklasse, um einen Trace zu den Aktivitäten für zeilenbasierte Operationen zu erstellen.
SCHED	Traceklasse für die Funktionen zur zentralen Zeitplanung. Diese Traceklasse gilt sowohl für klassische als auch für erweiterte Zeitpläne.	Verwenden Sie diese Traceklasse, um Fehler für Zeitplanbefehle, wie z. B. **DEFINE/UPDATE/QUERY SCHEDULE** oder **DEFINE ASSOCIATION**, zu beheben. Verwenden Sie diese Traceklasse auch zur Behebung von Problemen mit Hintergrundprozessen für die zentrale Zeitplanung, wie z. B. Zeitplanmanager und Zeitplanprompter.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
SESSION	Diese Traceklasse zeigt Informationen zu Sitzungen an, die mit dem Server verbunden sind, einschließlich aller Verben, die vom Server gesendet und empfangen wurden.	Diese Traceklasse wird für fehlerhafte Protokolle, Transaktionsverarbeitungsfehler oder für Fälle verwendet, in denen der Client gestoppt wurde und nicht antwortet.
SESSREMOTE	Erstellt einen Trace für die Kommunikation zwischen dem Server und dem Client während der Ausführung von NDMP-Sicherungs- und -Zurückschreibungsoperationen.	Diese Traceklasse wird verwendet, um NDMP-Sicherungs- oder -Zurückschreibungsoperationen zu identifizieren, die mithilfe des IBM Spectrum Protect-Web-Clients oder -Befehlszeilenclients eingeleitet werden.
SHRED	Diese Traceklasse zeigt Informationen zu Operationen zum Schreddern von Daten auf dem Server an.	Diese Traceklasse wird verwendet, um Probleme mit dem Schreddern von Daten zu diagnostizieren. Das Schreddern von Daten ist nur anwendbar, wenn mindestens ein Speicherpool auf dem Server einen Wert ungleich null für das Attribut SHRED aufweist. Aktivitäten, die sich auf das Schreddern von Daten beziehen, erfolgen hauptsächlich während der Ausführung der Befehle **EXPIRE INVENTORY**, **DELETE FILESPACE**, **DELETE VOLUME**, **MOVE DATA**, **MIGRATE** und **SHRED DATA**. Andere Traceklassen, die Aktivitäten zum Schreddern von Daten zurückmelden, sind BFDESTROY, DFDESTROY, DSALLOC, DSDEALLOC und CRCDATA.
SPI/SPID	Erstellt einen Trace für die NDMP-Protokollschnittstelle des Servers.	Die Traceklassen SPI und SPID werden verwendet, um Probleme zu identifizieren, die sich auf NDMP-Sicherungs- oder -Zurückschreibungsoperationen von NAS-Dateiservern beziehen. Diese Traceklassen sind für die Funktionen bestimmt, die das NDMP-Protokoll implementieren und mit einem NAS-Dateiserver kommunizieren. Die Traceklasse SPID stellt eine ausführlichere Traceerstellung bereit, einschließlich einer Traceerstellung für alle NDMP-Protokolldateisätze, die vom NAS-Dateiserver gesendet werden.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
SSLDATA	Detaillierter SSL-Trace (SSL = Secure Sockets Layer), der verwendet wird, um Informationen auf Byteebene zu Daten anzuzeigen, die zwischen dem Client für Sichern/Archivieren und dem Server gesendet oder empfangen werden.	Verwenden Sie die Traceklasse SSLDATA, um die Probleme mit fehlerhaften Sitzungsdaten zu beheben, die durch SSL verursacht werden können, das über die Serveroption SSLTCP oder SSLTCPADMIN ausgeführt wird. Da dies ein Trace auf Byteebene ist, kann ein großes Datenvolumen gesammelt werden.
SSLINFO	Allgemeiner SSL-Trace, der verwendet wird, um den Aufbau und die Kenndaten von SSL-Sitzungen zwischen dem Client für Sichern/Archivieren und dem Server anzuzeigen.	Verwenden Sie die Traceklasse SSLINFO, um Sitzungsverbindungs- und Handshakefehler zu beheben, die durch SSL verursacht werden können, das über die Serveroption SSLTCP oder SSLTCPADMIN ausgeführt wird. Diese Traceklasse kann zusammen mit den Traceklassen TCPINFO und SESSION verwendet werden.
TBREORG	Diese Traceklasse sammelt Informationen zu Aktivitäten bezüglich der Tabellen- und Indexreorganisation, die vom Server eingeleitet werden.	Verwenden Sie die Traceklasse TBREORG, um Probleme mit den vom Server eingeleiteten Reorganisationsaktivitäten zu beheben.
TBLMGR	Erstellt einen Trace zu Aktivitäten für tabellenbasierte Operationen.	Verwenden Sie die Traceklasse TBLMGR, um tabellenbasierte Operationen, wie z. B. Tabellenregistrierung, Öffnen von Tabellen und Schließen von Tabellen, anzuzeigen.
TCP	Diese Traceklasse sammelt Informationen zu TCP/IP, das zwischen dem Client und dem Server oder Speicheragenten verwendet wird. TCP ist eine zusammengefasste Traceklasse. Sie aktiviert TCPINFO und TCPERROR.	Verwenden Sie diese Traceklasse, um Sitzungsverbindungsfehler oder Probleme mit fehlerhaften Daten zu beheben, die durch das Netz verursacht werden können.
TCPDATA	Der detaillierte TCP/IP-Trace wird verwendet, um Informationen auf Byteebene zu Daten anzuzeigen, die gesendet oder empfangen werden.	Verwenden Sie diese Traceklasse, um Probleme mit fehlerhaften Sitzungsdaten zu beheben, die durch das Netz verursacht werden können.
TCPINFO	Der allgemeine TCP/IP-Trace wird verwendet, um die Konfiguration und die Kenndaten von TCP/IP auf dem Server oder Speicheragenten anzuzeigen.	Verwenden Sie diese Traceklasse, um Probleme mit fehlerhaften Sitzungsdaten zu beheben, die durch das Netz verursacht werden können.
TEC	Diese Traceklasse stellt Informationen zu den Ereignissen bereit, die an einen TEC-Server gesendet werden. Diese Ereignisse entsprechen dem Ereignisempfänger TIVOLI.	Verwenden Sie diese Traceklasse, um Verbindungsprobleme zu beheben, die bei der TEC-Ereignisprotokollierung auftreten.

Tabelle 10. Traceklassen für den Server oder Speicheragenten (Forts.)

Traceklassen	Beschreibung	Verwendung
TOC	Diese Traceklasse wird für die TOC-Komponente (Table Of Contents = Inhaltsverzeichnis) verwendet, die während der Ausführung von NDMP-Operationen auf Dateiebene eingesetzt wird. TOC ist eine zusammengefasste Traceklasse, die TOCBUILD, TOCLOAD, TOCREAD und TOCUTIL aktiviert.	Verwenden Sie diese Traceklasse, um Probleme während der Ausführung von NDMP-Operationen auf Dateiebene, wie z. B. eine NDMP-Sicherung mit dem Parameter TOC=YES oder eine NDMP-Zurückschreibung mit dem Parameter **FILELIST**, zu beheben.
TOCBUILD	TOC-Erstellungsfunktionen (Tables Of Contents = Inhaltsverzeichnis).	Verwenden Sie diese Traceklasse, um Probleme während einer NDMP-Sicherung mit dem Parameter **TOC=YES** zu beheben.
TOCLOAD	TOC-Ladefunktionen (Table Of Contents = Inhaltsverzeichnis).	Verwenden Sie diese Traceklasse, um Probleme beim Anzeigen von Dateien und Verzeichnissen in der Client-GUI zu beheben.
TOCREAD	TOC-Lesefunktionen (Table Of Contents = Inhaltsverzeichnis).	Verwenden Sie diese Traceklasse, um Probleme während der Ausführung eines Befehls **QUERY TOC** oder beim Laden eines Inhaltsverzeichnisses zum Anzeigen von Dateien und Verzeichnissen in der Client-GUI zu beheben.
TOCUTIL	TOC-Dienstprogrammfunktionen (Table Of Contents = Inhaltsverzeichnis).	Verwenden Sie diese Traceklasse, um Fehler zu beheben, die sich auf die TOC-Komponenteninitialisierung oder die TOC-Aufbewahrungsdauer beziehen.
UNICODE	Diese Traceklasse zeigt Informationen zu Codepagekonvertierungen und Unicode-Dateibereichsoperationen an.	Verwenden Sie diese Traceklasse, um Fehler zu beheben, die sich auf die Codepagekonvertierung oder auf Unicode-Dateibereichsprobleme beziehen.
XI	Diese Traceklasse zeigt allgemeine Informationen zu den Befehlen **IMPORT** und **EXPORT** an.	Verwenden Sie diese Traceklasse, um Fehler zu beheben, die sich auf die Befehle **IMPORT** und **EXPORT** beziehen.

Befehle SHOW für den Server oder Speicheragenten

Befehle **SHOW** sind nicht unterstützte Diagnosebefehle, die verwendet werden, um Informationen zu speicherinternen Steuerstrukturen und andere Laufzeitattribute anzuzeigen. Die Befehle **SHOW** werden von der Entwicklung und dem Service nur als Diagnosetools verwendet. Für den Client für Sichern/Archivieren sind mehrere Befehle **SHOW** vorhanden.

Abhängig von den Informationen, die ein Befehl **SHOW** anzeigt, kann es Instanzen geben, bei denen sich die Informationen ändern, oder kann es Fälle geben, in denen die Informationen zur Folge haben, dass die Anwendung (Client, Server oder Speicheragent) gestoppt wird. Die Befehle **SHOW** dürfen nur nach einer entsprechen-

den Empfehlung des IBM Software Support verwendet werden. Die hier aufgeführten Befehle **SHOW** sind ein Teil der verfügbaren Befehle **SHOW**.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten

Befehl SHOW	Beschreibung	Empfehlung
AGGREGATE	Zeigt Informationen zu einem zusammengefassten Objekt in der Serverspeicherhierarchie an. Die Syntax ist **SHOW AGGRegate aggr***ID-hoch* aggr*ID-tief*. aggr*ID-hoch* und aggr*ID-tief* sind die höchstwertigen und niedrigstwertigen 32-Bit-Wörter der 64-Bit-Aggregat-ID des Aggregats, das abgefragt wird.	Geben Sie diesen Befehl aus, um das Vorhandensein von logischen Dateien zu bestimmen, die in einem zusammengefassten Objekt in der Speicherhierarchie des Servers gespeichert sind. Der Offset, die Länge und der aktive Status von Sicherungsdateien werden für Dateien innerhalb des Aggregats angezeigt. Sie können diesen Befehl bei Problemen mit dem Zurückschreiben oder Abrufen von Dateien, mit der Datenverfallsverarbeitung oder Datenversetzung, mit dem Sichern von primären Speicherpools, mit dem Kopieren von aktiven Daten in Pools für aktive Daten oder mit dem Prüfen von Datenträgern ausgeben.
ASQUEUED	Zeigt die Warteschlange für Mountpunkte an. Die Syntax ist **SHOW ASQueued**.	Um ein Laufwerk, eine Clientsitzung oder einen Serverprozess verwenden zu können, müssen Sie zuerst einen Mountpunkt anfordern. Die Mountpunktverwaltung auf dem Server ermöglicht es, auf einen Mountpunkt wartende Sitzungen oder Prozesse in eine Warteschlange einzureihen, wenn mehr Mountpunkte benötigt werden, als verfügbar sind. Mit diesem Befehl kann der Status einer Mountpunktanforderung bestimmt werden. Dies gilt besonders dann, wenn eine Sitzung oder ein Prozess gestoppt wurde und auf einen Mountpunkt wartet.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
ASVOL	Zeigt zugeordnete Datenträger an. Die Syntax ist **SHOW ASVol**.	Während sequenzielle Datenträger für die Verwendung durch eine Sitzung oder einen Prozess zugeordnet sind, werden sie in einer speicherinternen Liste verfolgt. Sie können diese Liste aufrufen, um den Status von verwendeten Datenträgern und Stopps oder Sperren zu bestimmen, bei denen eine Sitzung oder ein Prozess dauerhaft auf einen Datenträger wartet oder einen Datenträger belegt und auf etwas anderes wartet.
BFOBJECT	Zeigt die folgenden Informationen in der Serverspeicherhierarchie an: • Den aktiven/inaktiven Status von logischen Dateien innerhalb eines Aggregats • Den Offset/die Länge von logischen Dateien innerhalb eines Aggregats • Den aktiven Status oder die Eignerbitdatei-ID von logischen Dateien innerhalb eines Aggregats • Die Verbindungsbitdatei-ID, wenn der deduplizierte Speicherbereich mit einem anderen Speicherbereich verbunden ist Die Syntax ist **SHOW BFObject**.	Mit diesem Befehl können Sie das Vorhandensein und die Attribute eines Bitdateiobjekts in der Speicherhierarchie des Servers bestimmen. Sie können diesen Befehl bei Problemen mit dem Zurückschreiben, dem Abrufen, der Verfallsverarbeitung oder der Prüfung des Objekts ausgeben.
CMD DEDUPDELETEINFO	Zeigt den Status von Threads für das Löschen im Hintergrund für dereferenzierte deduplizierte Objekte an.	Geben Sie diesen Befehl aus, um den Status des Prozesses zum Löschen im Hintergrund für deduplizierte Objekte zu überprüfen. Wenn eine Datei aus einem deduplizierten Speicherpool gelöscht oder versetzt wird, werden die Speicherbereiche in die Warteschlange eines Hintergrundprozessors für versuchtes Entfernen aus dem Speicherpool gestellt. Dieser Befehl ist nützlich, um den Umfang der eingereihten Speicherbereiche und den Status jedes Löschthreads zu überprüfen.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
CONFIGURATION	Der Befehl **CONFIGURATION** ist ein SHOW-Zusammenfassungsbefehl, mit dem tatsächlich viele verschiedene SHOW-Befehle und Abfragen ausgegeben werden. Die Syntax ist **SHOW CONFIGuration**.	Geben Sie diesen Befehl aus, um allgemeine Konfigurationsdaten und andere Informationen zu dem Server für den IBM Service bereitzustellen.
DB2CONNECTIONS	Der Befehl DB2CONNECTIONS zeigt die definierten DB2-Verbindungen aus den verschiedenen Verbindungspools an. Dieser Befehl erfordert keine weiteren Parameter. Die Syntax ist **SHOW DB2CONnections**.	Geben Sie diesen Befehl aus, um anzuzeigen, wie viele DB2-Verbindungen insgesamt und in einem bestimmten Pool definiert, im Gebrauch und frei sind.
DB2TABLES	Der Befehl DB2TABLES zeigt die registrierten Tabellen und ihre Spaltenattribute an. Dieser Befehl erfordert keine weiteren Parameter. Die Syntax ist **SHOW DB2TABles**.	Geben Sie diesen Befehl aus, um die registrierten Tabellen und ihre Spaltenattribute anzuzeigen.
DBVARS	Zeigt globale Attribute für die Datenbank an. Die Syntax ist **SHOW DBVars**.	Geben Sie diesen Befehl aus, um den aktuellen Status und die Attribute der Serverdatenbank anzuzeigen.
DEDUPOBJECT	Zeigt Datendeduplizierungsinformationen für Dateien an. Wenn Sie diesen Befehl ausgeben, müssen Sie den Parameter **objectID** angeben. Geben Sie den Befehl **SHOW VERSION** aus, um den Wert dieses Parameters zu bestimmen. Die Syntax ist **SHOW DEDUPObject**.	Geben Sie diesen Befehl aus, um Datendeduplizierungsinformationen anzuzeigen, wie z. B.: • Die Bitdatei-ID für jeden Speicherbereich • Die Eignerbitdatei-ID • Den Offset und die Länge der Eignerbitdatei • Den Digesttyp und Wert des Datendeduplizierungsobjekts
DEVCLASS	Zeigt Informationen zu Einheitenklassen an. Die Syntax für diesen Befehl ist **SHOW DEVCLass**.	Geben Sie diesen Befehl aus, um den Status von zugeordneten Laufwerken, Einheitenklassenattribute und andere Informationen anzuzeigen. Dieser Befehl wird oft verwendet, um Probleme mit Einheiten oder Sperren beim Warten auf ein Laufwerk, ein Kassettenarchiv oder einen Datenträger zu diagnostizieren. Der Befehl **SHOW LIBRARY** stellt ebenfalls wichtige ergänzende Informationen zu Laufwerken und Kassettenarchiven bereit.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
GROUPLEADERS	Zeigt alle Sicherungsgruppenleiter für ein Objekt im Serverbestand an. Die Syntax ist **SHOW GROUPLeaders** *ObjID-hoch ObjID-tief*. *ObjID-hoch* und *ObjID-tief* sind die höchstwertigen und niedrigstwertigen 32-Bit-Wörter der 64-Bit-Objekt-ID des Objekts, das abgefragt wird. Das höchstwertige Wort ist optional; falls nicht angegeben, wird der Wert Null angenommen. Das Objekt muss ein Sicherungsobjekt sein.	Geben Sie diesen Befehl aus, um die Sicherungsgruppenbeziehungen eines Objekts im Serverbestand zu bestimmen. Sie können diesen Befehl bei Problemen mit dem Zurückschreiben, dem Abrufen, der Verfallsverarbeitung oder der Prüfung des Objekts ausgeben.
GROUPMEMBERS	Zeigt alle Sicherungsgruppenmitglieder für ein Objekt im Serverbestand an. Die Syntax ist **SHOW GROUPMembers** *ObjID-hoch ObjID-tief. ObjID-hoch* und *ObjID-tief* sind die höchstwertigen und niedrigstwertigen 32-Bit-Wörter der 64-Bit-Objekt-ID des Objekts, das abgefragt wird. Das höchstwertige Wort ist optional; falls nicht angegeben, wird der Wert Null angenommen. Das Objekt muss ein Sicherungsobjekt sein.	Geben Sie diesen Befehl aus, um die Sicherungsgruppenbeziehungen eines Objekts im Serverbestand zu bestimmen. Sie können diesen Befehl bei Problemen mit dem Zurückschreiben, dem Abrufen, der Verfallsverarbeitung oder der Prüfung des Objekts ausgeben.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
INVOBJECT	Zeigt Informationen zu einem Bestandsobjekt im Server an. Die Syntax ist **SHOW INVObject** *ObjID-hoch ObjID-tief*. *ObjID-hoch* und *ObjID-tief* sind die höchstwertigen und niedrigstwertigen 32-Bit-Wörter der 64-Bit-Objekt-ID des Objekts, das abgefragt wird. Das höchstwertige Wort ist optional; falls nicht angegeben, wird der Wert Null angenommen. Das Objekt kann ein Sicherungsobjekt, Archivierungsobjekt, speicherverwaltetes Objekt usw. sein.	Geben Sie diesen Befehl aus, um das Vorhandensein und die Attribute eines Objekts im Serverbestand zu bestimmen. Sie können diesen Befehl bei Problemen mit dem Zurückschreiben, dem Abrufen, der Verfallsverarbeitung oder der Prüfung des Objekts ausgeben. Der Befehl **INVOBJECT** gibt die folgenden Informationen zurück: • Neue Informationen für Objekte, die durch den Aufbewahrungsschutz für Archivierung geschützt sind • Informationen darüber, ob das Archivierungsobjekt den Status 'Löschen unzulässig' hat • Informationen darüber, ob das Objekt die ereignisgesteuerte Aufbewahrungsdauer verwendet
LIBINVENTORY	Zeigt den aktuellen Status des Kassettenarchivbestands für das angegebene Kassettenarchiv an. Die Syntax ist **SHOW LIBINVentory** *Kassettenarchivname*. Dabei ist *Kassettenarchivname* optional. Falls nicht angegeben, gibt der Befehl die Informationen zum Bestand für alle Kassettenarchive zurück.	Geben Sie diesen Befehl aus, wenn ein Problem mit den Informationen zum Kassettenarchivbestand auftritt. Der Befehl zeigt die aktuellen speicherinternen Merkmale des Kassettenarchivbestands an.
LIBRARY	Verwenden Sie den Befehl **LIBRARY**, um den aktuellen Status des angegebenen Kassettenarchivs und seiner Laufwerke anzuzeigen. Die Syntax ist **SHOW LIBRary** *Kassettenarchivname*. Dabei ist *Kassettenarchivname* optional. Falls nicht angegeben, gibt der Befehl Informationen für alle Kassettenarchive zurück.	Dieser Befehl ist nützlich, um eine schnelle Anzeige aller speicherinternen Informationen zu einem Kassettenarchiv und seinen Laufwerken zu erstellen. Diese Ausgabe kann für jedes Problem erstellt werden, das sich auf Kassettenarchive oder Laufwerke bezieht (z. B. Mountprobleme).

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
LOCK	Zeigt Sperreninhaber und wartende Threads an. Die Syntax ist **SHOW LOCK**.	Der Server und der Speicheragent verwenden Sperren als Mechanismus, um den Zugriff und die Aktualisierungen für Informationen und andere Konstrukte zu serialisieren. Diese Informationen werden verwendet, um Stopps oder andere Probleme bei Ressourcenkonflikten zu diagnostizieren.
MEMTREND	Mit dem Befehl **MEMTREND** wird der vom Server verwendete Speicher in Megabyte zurückgemeldet. Er wird in stündlichen Intervallen für die letzten 50 Stunden aufgezeichnet. Dieser Befehl ist im Server-Code festgelegt. Er kann nicht konfiguriert werden. Der Befehl zeigt außerdem ein Histogramm an, um den Nutzungstrend zu visualisieren. Die Syntax ist **SHOW MEMTREnd**.	Geben Sie diesen Befehl aus, um zu bestimmen, ob der Server ein Speicherleck hat. Wenn die Speicherbelegung ständig zunimmt, ist möglicherweise ein Speicherverlust aufgetreten. Damit die Messwerte gültig sind, muss die Messperiode (die letzten 50 Stunden) eine normale, stabile Serveraktivität darstellen. Die zurückgemeldete Belegung stellt die Speichermenge dar, die interne Serverroutinen von den Pseudokernelspeicherroutinen anfordern. Sie stellt NICHT die gesamte Speichermenge dar, die vom Server verwendet wird. Mit diesem Befehl kann der Speichernutzungstrend des Servers ermittelt werden.
MP	Zeigt Mountpunkte an. Die Syntax ist **SHOW MP**.	Geben Sie diesen Befehl aus, um zu bestimmen, welcher Datenträger von einem Mountpunkt verwendet wird, und andere Attribute für die zugeordneten Mountpunkte anzuzeigen. **SHOW LIBRARY** und **SHOW DEVCLASS** stellen nützliche ergänzende Informationen bereit, indem sie den aktuellen Status von Laufwerken und die aktuelle Anzahl von Mountpunkten für die Einheitenklasse anzeigen.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
NASDEV	Zeigt die SCSI-Einheiten an, die an einen NAS-Dateiserver angeschlossen sind, dem eine Definition als NAS-Einheit zum Versetzen von Daten zugeordnet ist. Die Syntax ist **SHOW NASDev**.	Erstellen Sie eine NDMP-Verbindung (NDMP = Network Data Management Protocol) zum angegebenen NAS-Dateiserver und zeigen Sie die angeschlossenen SCSI-Einheiten auf dem Dateiserver an. Dieser Befehl erfordert nur einen NAS-Knoten und eine Definition für eine Einheit zum Versetzen von Daten.
NASFS	Zeigt die Dateisysteme auf einem NAS-Dateiserver an, dem eine Definition als NAS-Einheit zum Versetzen von Daten zugeordnet ist. Die Syntax ist **SHOW NASFs**.	Erstellen Sie eine NDMP-Verbindung zum angegebenen NAS-Dateiserver und zeigen Sie die Dateisysteme an, die auf dem Dateiserver definiert sind. Alle angezeigten Dateisysteme können von IBM Spectrum Protect gesichert werden. Dieser Befehl erfordert nur einen NAS-Knoten und eine Definition für eine Einheit zum Versetzen von Daten.
NASINFORMATION	Zeigt Konfigurationsdaten zu dem NAS-Dateiserver an, dem eine Definition als NAS-Einheit zum Versetzen von Daten zugeordnet ist. Die Syntax ist **SHOW NASInformation**.	Erstellen Sie eine NDMP-Verbindung zum angegebenen NAS-Dateiserver und zeigen Sie allgemeine Konfigurationsdaten an, die vom Dateiserver abgerufen werden. Dieser Befehl ist nützlich, um grundlegende Kommunikationsfehler, wie z. B. Authentifizierungsfehler, mit NAS-Dateiservern zu identifizieren. Dieser Befehl erfordert nur einen NAS-Knoten und eine Definition für eine Einheit zum Versetzen von Daten.
NASWORKLOAD	Zeigt die Arbeitslast von NAS-Dateien an, die für alle IBM Spectrum Protect-Operationen verwendet werden. Die Syntax ist **SHOW NASWorkload**.	Geben Sie diesen Befehl aus, um die Arbeitslast der Back-End-Datenversetzung sowie von Sicherungs- und Zurückschreibungsoperationen zu bestimmen.
REPLICATION	Zeigt alle bekannten Replikationsserver und ihre global eindeutigen IDs sowie alle aktiven Replikationsprozesse an. Die Prozesse können die einzelnen Statistiken für jeden Dateibereich und den Status jeder Replikationssitzung einschließen.	Geben Sie diesen Befehl aus, wenn die Replikation keinen Fortschritt zeigt oder die Replikation nicht korrekt arbeitet.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
RESQUEUE	Zeigt die Ressourcenwarteschlange an. Die Syntax ist **SHOW RESQueue**.	Verwenden Sie die Ressourcenwarteschlange, um allgemeine Ressourcen auf dem Server zu überwachen. Wenn eine Ressource gestoppt ist oder eine Ressource unverhältnismäßig lange belegt ist, brechen die Ressourcenüberwachungsalgorithmen für den Server den Ressourcenbenutzer ab. Dieser Befehl wird verwendet, um Informationen zu Transaktionen, Sperren und anderen Ressourcen anzuzeigen, die von einem Speicheragenten auf dem Datenbankserver verwendet werden, für dessen Verwendung er konfiguriert ist.
SESSIONS	Zeigt Informationen zu Sitzungen an, die mit dem Server oder Speicheragenten verbunden sind. Die Syntax ist **SHOW SESSions**.	Geben Sie diesen Befehl aus, um Stopps oder andere allgemeine Sitzungsprobleme zu diagnostizieren, während eine Sitzung noch mit dem Server verbunden ist. Dieser Befehl ist auch in Fällen nützlich, in denen eine Sitzung abgebrochen wurde, aber noch mit **QUERY SESSION** angezeigt wird.
SLOTS	Zeigt den aktuellen Status der Schachtinformationen für das angegebene Kassettenarchiv an (z. B. welche Datenträger sich in dem Kassettenarchiv und in welchen Schächten befinden). Die Syntax ist **SHOW SLOTS** *Kassettenarchivname*.	Die angezeigten Informationen werden direkt aus der Kassettenarchivhardware in speicherinternen Werten gespeichert. Mit ihrer Hilfe kann bestimmt werden, ob diese Informationen nicht synchron oder falsch sind oder ob die von der Kassettenarchivhardware selbst zurückgegebenen Werte falsch sind. Alternativ können Sie diesen Befehl ausgeben, um die Laufwerkelementnummern für ein SCSI-Kassettenarchiv zu bestimmen, wenn **QUERY SAN** für ein bestimmtes Kassettenarchiv nicht verfügbar ist.
SSPOOL	Zeigt Informationen zu Speicherpools an. Die Syntax ist **SHOW SSPool**.	Geben Sie diesen Befehl aus, um den Status und die Attribute von definierten Speicherpools anzuzeigen.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
THREADS	Zeigt Informationen zu allen Threads an, die dem Server bekannt sind. Die Syntax ist **SHOW THReads**. **Wichtig:** Bei einigen Betriebssystemen (z. B. HP) werden die zurückgemeldeten Informationen ohne serielle Anordnung abgerufen. Auf einem ausgelasteten System können Informationen inkonsistent sein. Mehrere Threads können zurückmelden, dass sie denselben Mutex sperren, oder ein Thread kann zurückmelden, dass er auf einen Mutex wartet, der von einem anderen Thread gesperrt wird, der die Sperre nicht anfordert.	Der Server zeigt Informationen zu jedem Thread an. Dazu gehören normalerweise die IBM Spectrum Protect-Thread-ID, die System-Thread-ID, der Threadname, die gesperrten Mutexe (falls zutreffend) und der Mutex oder die Bedingung, auf den bzw. die gewartet wird (falls zutreffend). Dieser Befehl ist plattformspezifisch, d. h., für jede Plattform können etwas andere Informationen bereitgestellt werden. Sie können diesen Befehl ausgeben, wenn der Server oder ein bestimmter Serverprozess gestoppt wurde, um zu bestimmen, ob Threads auf Ressourcen warten, die von einem anderen Thread gesperrt werden.
TOCSETS	Zeigt alle Inhaltsverzeichnisgruppen an, die dem Server bekannt sind. Die Syntax ist **SHOW TOCSets DELETE**=*Gruppennummer* **TOUCH**=*Gruppennummer*. Mit dem Parameter **DELETE** wird die angegebene Inhaltsverzeichnisgruppennummer gelöscht. Mit dem Parameter **TOUCH** wird das Datum der letzten Verwendung der angegebenen Inhaltsverzeichnisgruppennummer aktualisiert. Eine Inhaltsverzeichnisgruppe wird für den Aufbewahrungszeitraum aufbewahrt, der auf das Datum der letzten Verwendung folgt (siehe Befehl **SET TOCRETENTION**).	Eine Inhaltsverzeichnisgruppe wird während der Ausführung von NDMP-Operationen auf Dateiebene verwendet. Während einer NDMP-Sicherung mit dem Parameter TOC=YES wird ein Inhaltsverzeichnis in der Serverdatenbank erstellt. Während einer Zurückschreibung können ein oder mehrere Inhaltsverzeichnisse in die Serverdatenbank geladen werden, um Datei- und Verzeichnisnamen für die Client-GUI bereitzustellen. Mit diesem Befehl werden der Status der Inhaltsverzeichnisgruppe (z. B. 'wird erstellt' oder 'wird geladen') und der temporäre Datenbankbereich angezeigt, der von jeder Inhaltsverzeichnisgruppe verwendet wird. Sie können diesen Befehl ausgeben, wenn Sie Probleme mit einer NDMP-Sicherung mit dem Parameter **TOC=YES** haben oder Probleme mit der Zurückschreibung von Dateien aus einer NDMP-Sicherung haben oder wenn Inhaltsverzeichnisgruppen in der Serverdatenbank zu lange oder nicht lange genug aufbewahrt werden.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
TOCVARS	Zeigt Informationen zur Inhaltsverzeichniskomponente des Servers an. Die Syntax ist **SHOW TOCVars**.	Geben Sie diesen Befehl aus, um den Status der Inhaltsverzeichniskomponente zu bestimmen. Sie können diesen Befehl ausgeben, wenn Sie Probleme mit einer NDMP-Sicherung mit dem Parameter **TOC=YES** haben oder Probleme mit der Zurückschreibung von Dateien aus einer NDMP-Sicherung haben.
TXNTABLE	Zeigt Informationen zu Transaktionen an, die sich in der Liste der verwendeten Transaktionen auf dem Server befinden. Die Syntax ist **SHOW TXNTable**.	Die Transaktionen, die von diesem Befehl gefiltert werden, werden von Serverprozessen, Sitzungen oder anderen Operationen verwendet, um Informationen aus der Datenbank zu lesen, Aktualisierungen an der Datenbank vorzunehmen (z. B. Informationen einfügen, aktualisieren oder löschen) oder Sperren zu verwalten. Diese Informationen sind nützlich, um Stopps oder andere transaktionsbezogene Fehler zu diagnostizieren, während die Transaktion noch auf dem Server offen ist.
VALIDATE LANFREE	Überprüft, ob die Definitionen auf dem Server vorhanden sind, damit ein Client LAN-unabhängige Datenversetzungsoperationen ausführen kann. In Fällen, in denen diese Definitionen nicht vorhanden oder falsch sind, kann es schwierig sein festzustellen, ob die LAN-unabhängige Umgebung ordnungsgemäß konfiguriert ist. Die Syntax ist **VALIDATE LANFREE** *Knotenname Speicheragent*. **Anmerkung:** Der Befehl **VALIDATE LANFREE** hat den Befehl **SHOW LANFREE** ersetzt.	Dieser Befehl überprüft alle möglichen Zielspeicherpools für diesen Clientknoten und meldet zurück, ob der Speicherpool LAN-unabhängige Datenversetzungsoperationen ausführen kann.
VERSIONS	Geben Sie den Befehl **SHOW VERSIONS** aus, um eine **objectID** abzurufen. Die **objectID** ist erforderlich, um den Befehl **SHOW DEDUPOBJECT** auszugeben. Die Syntax ist **SHOW Versions**.	Geben Sie diesen Befehl aus, um Objekt-IDs anzuzeigen.

Tabelle 11. Befehle SHOW für den Server oder Speicheragenten (Forts.)

Befehl SHOW	Beschreibung	Empfehlung
VOLINUSE	Zeigt an, ob sich der angegebene Datenträger in der Liste der verwendeten Datenträger des Servers befindet. Der Befehl **VOLINUSE** zeigt zusätzliche Informationen an, die nützlich sein können. Dazu gehören Informationen darüber, ob der Datenträger für das Entfernen aus der Liste der verwendeten Datenträger ansteht. Die Syntax ist **SHOW VOLINUSE** *Datenträgername*. Wenn der Datenträger aus der Liste der verwendeten Datenträger entfernt werden muss, können Sie den folgenden Parameter angeben, um den Datenträger aus der Liste zu entfernen: **SHOW VOLINUSE** *Datenträgername* REMOVE=YES.	Geben Sie diesen Befehl aus, um zu bestimmen, ob sich ein Datenträger in der Liste der verwendeten Datenträger befindet und, falls erforderlich, den Datenträger aus dieser Liste zu entfernen. Operationen, die diesem Datenträger zugeordnet sind, können fehlschlagen, wenn der Datenträger aus der Liste der verwendeten Datenträger entfernt wird.

Trace für den IBM Spectrum Protect-Einheitentreiber aktivieren

Die Tracefunktion ist für den IBM Spectrum Protect-Einheitentreiber verfügbar. Für den IBM Spectrum Protect-Einheitentreiber kann ein Trace über die Serverkonsole, einen Verwaltungsclient oder über eine Shell erstellt werden, die auf dem System ausgeführt wird, auf dem der Einheitentreiber installiert ist.

Die Anweisungen für die Traceerstellung gelten für alle Plattformen, auf denen der IBM Spectrum Protect-Einheitentreiber unterstützt wird. Für Einheiten, die andere Einheitentreiber als den IBM Spectrum Protect-Einheitentreiber verwenden, werden Informationen zur Tracefunktion und Anweisungen zur Traceerstellung für diese Einheitentreiber vom Einheitenhersteller bereitgestellt.

Zugehörige Verweise:

„Trace über die Serverkonsole durchführen"

„Trace für Daten über eine Befehlsshell für AIX und Windows durchführen" auf Seite 153

Trace über die Serverkonsole durchführen

Um ein Trace für den Treiber über den Server durchzuführen, müssen Sie zuerst die entsprechenden Befehle ausgeben.

Geben Sie die Befehle **TRACE ENABLE** und **TRACE BEGIN** aus, um einen Trace für den Treiber über den Server durchzuführen.

Der IBM Spectrum Protect-Einheitentreiber besteht tatsächlich aus zwei Treibern, nämlich einem Treiber für Kassettenwechsler im Kassettenarchiv und einem Treiber für Bandeinheiten. Sie können den Treiber auswählen, für den ein Trace durchgeführt werden soll. Die folgende Syntax gilt für den Befehl:

DDTRACE START [LIBRARYDD | TAPEDD]
[flags=EE |, FULL |, SYSLOG | BASE]
DDTRACE GET [LIBRARYDD | TAPEDD]
DDTRACE END [LIBRARYDD | TAPEDD]

Die folgenden Optionen sind verfügbar:

START Aktiviert die Tracefunktion und schreibt den Trace auf der Basis des Standardwerts oder der angegebenen FLAGS-Option in einen Hauptspeicherpuffer.

GET Schreibt den Hauptspeicherpuffer in die Datei, die mit dem Serverbefehl **TRACE BEGIN** angegeben wurde.

END Stoppt das Schreiben des Trace in den Hauptspeicherpuffer, aber bereinigt nicht den Inhalt des Puffers, sodass Sie END vor GET ausführen können.

LIBRARYDD
Erstellt einen Trace für den Einheitentreiber, der Kassettenwechsler im Kassettenarchiv steuert.

TAPEDD Erstellt einen Trace für den Einheitentreiber, der Bandlaufwerke steuert.

Für die oben aufgelisteten Optionen können Sie einen beliebigen Einheitentreiber oder den Treiber der Kassettenarchiveinheit und einen der beiden anderen Einheitentreiber angeben. Diese werden durch Leerzeichen getrennt. Beispiel:

DDTRACE START TAPEDD - Startet die Traceerstellung für den Einheitentreiber, der Bandlaufwerke steuert.

DDTRACE START LIBRARYDD - Startet die Traceerstellung für den Einheitentreiber, der Kassettenwechsler im Kassettenarchiv steuert.

DDTRACE START LIBRARYDD TAPEDD - Erstellt einen Trace sowohl für das Kassettenarchiv als auch für die Bandlaufwerke.

Unabhängig davon, welche dieser Optionen Sie verwenden, geben Sie dieselben Optionen für alle Befehle in der Start-Get-End-Serie an.

Der Parameter **FLAGS** ist optional und ist normalerweise nicht erforderlich. Die folgenden Werte gelten für den Parameter **FLAGS**:

EE Erstellt einen Trace für alle Einstiege und Ausstiege der Einheitentreiberroutine.

FULL Aktiviert eine erweiterte Tracefunktion für die Fehlerbehebung und stellt mehr Details bereit. Da die Größe des Hauptspeicherpuffers festgelegt ist, wird jedoch für weniger Ereignisse ein Trace erstellt. Erstellt keinen Trace für Routineneinstiegs- und -ausstiegspunkte.

SYSLOG
Auf einigen Plattformen werden mit SYSLOG die Traceanweisungen nicht nur in den Hauptspeicherpuffer, sondern auch in das Systemprotokoll geschrieben. Dies ist besonders bei der Fehlerbehebung für Kernelstopps oder beim Umbruch des Trace im Hauptspeicherpuffer nützlich.

BASE Der Wert BASE ist der Standardwert und kann mit keinen anderen Flags angegeben werden. Er wird nur verwendet, um die Flags EE, FULL und SYSLOG zu inaktivieren, ohne die Tracefunktion zu inaktivieren.

Trace für Daten über eine Befehlsshell für AIX und Windows durchführen

AIX Windows

Mit dem Standalone-Dienstprogramm 'ddtrace' werden die Serverbefehle **DDTRACE** exakt imitiert.

Das Standalone-Dienstprogramm 'ddtrace' wird im Verzeichnis für Einheiten installiert. Hierbei handelt es sich um dasselbe Verzeichnis wie für die Dienstprogramme 'mttest', 'lbtest' und 'optest'. Die Syntax und Optionen sind mit dem Serverbefehl **DDTRACE** identisch. Beispiel:

`$ ddtrace start librarydd tapedd flags=EE` - Traceerstellung für die Speicherarchiv- und Bandtreiber starten und zusätzlichen Eingangs-/Ausgangstrace abrufen.

`$ ddtrace get librarydd tapedd` - Den Trace aus dem Speicher abrufen und in die Datei ddtrace.out schreiben.

`$ ddtrace end librarydd tapedd` - Traceerstellung im Speicher stoppen.

Dieses Standalone-Dienstprogramm wird hauptsächlich verwendet, wenn für den Treiber während der IBM Spectrum Protect-Serverinitialisierung ein Trace durchgeführt werden muss. Das Dienstprogramm 'ddtrace' schreibt den Hauptspeicherpuffer in die Datei „ddtrace.out" im aktuellen Verzeichnis. Wenn die Datei vorhanden ist, wird er an die Datei angehängt, und die Datei wird nicht überschrieben.

Trace zur Erkennung eines Codepagekonvertierungsfehlers durchführen

Der IBM Spectrum Protect-Server verwendet Betriebssystemfunktionen für die Konvertierung zwischen Unicode und der Server-Codepage. Wenn das System nicht korrekt konfiguriert ist, schlägt die Konvertierung fehl.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um weitere Informationen zu dem Fehler zu erhalten:

1. Starten Sie die Tracefunktion für die Traceklasse UNICODE.
2. Wiederholen Sie die Aktion, die die Fehlernachricht zur Folge hatte.
3. Überprüfen Sie die Readme-Datei auf alle plattformspezifischen Voraussetzungen für die Spracheninstallation.
4. Stellen Sie sicher, dass die durch die Problemcodepages angegebenen Ländereinstellungen und alle in der Readme-Datei aufgelisteten Voraussetzungen installiert sind.

Trace für Clientdaten durchführen

Sie können die Tracefunktion für den Client oder die Anwendungsprogrammierschnittstelle (API) für den Client aktivieren, indem Sie die Clientoptionsdatei ändern.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Tracefunktion für den Client oder die Client-API zu aktivieren:

Vorgehensweise

1. Bestimmen Sie in der folgenden Tabelle die Traceklassen, die aktiviert werden sollen:

Name der Traceklasse	Beschreibung	Verwendung	Weitere Hinweise
SERVICE	Allgemeine Verarbeitungsinformationen für den Client anzeigen.	In vielen Fällen nützlich. Im Allgemeinen für fehlerhafte Protokolle, Transaktionsverarbeitungsfehler oder in Fällen empfohlen, in denen der Client gestoppt wurde und nicht antwortet.	
VERBINFO	Informationen erfassen, die das von IBM Spectrum Protect verwendete Client/Server-Protokoll betreffen.	Zur Ausführung des Debuggers für fehlerhafte Protokolle, Transaktionsverarbeitungsfehler oder in Fällen, in denen der Client gestoppt wurde und nicht antwortet.	
VERBDETAIL	Detaillierte Informationen erfassen, die das von IBM Spectrum Protect verwendete Client/Server-Protokoll betreffen. Damit werden interne Hauptspeicherpuffer angezeigt, die die vom Client gesendeten und empfangenen Verben enthalten.	Zur Ausführung des Debuggers für Probleme mit fehlerhaften Sitzungsdaten, die unter Umständen vom Netz verursacht wurden.	Damit wird ein großes Ausgabevolumen generiert.

2. Aktivieren Sie den Trace, indem Sie der Clientoptionsdatei den folgenden Text hinzufügen: `traceflag <Name der Traceklasse>`.

   Achtung: Bei *<Name der Traceklasse>* kann es sich um eine Liste mit durch Kommas getrennten Traceklassen handeln. Es könnte beispielsweise Folgendes angegeben werden: `traceflag service,verbinfo,verbdetail`.

3. Konfigurieren Sie den Start des Trace und die Ausgabe der Tracenachrichten in eine Datei, indem Sie der Clientoptionsdatei den folgenden Text hinzufügen: `tracefile <Dateiname>`.

4. Führen Sie die Operation aus, die den Fehler verursacht.

   Tipp: Die Tracefunktion kann auch konfiguriert und gestartet werden, indem der Client über eine Eingabeaufforderung unter Angabe der oben aufgeführten Flags aufgerufen wird. Beispiel: `dsm -traceflags=service -tracefile=file.out`.

Trace-Flags für Client und Journaldämon

Um eine journalbasierte Sicherung auszuführen, müssen Sie den Journaldämonprozess verwenden. Dieser Prozess wird verwendet, um Dateisystemänderungen zu verfolgen und Änderungsjournaldatenbanken zu verwalten.

Der Journaldämon verwendet denselben Tracemechanismus wie der Client, aber die Traceeinstellungen werden wie folgt in der Journalkonfigurationsdatei (`tsmjbbd.ini`) angegeben:

```
[JournalSettings]
TraceFlags=all_jbb
;
; the following two settings allow tracefile segmentation
;
TraceMax=100
TraceSegMax=1
tracefile=tracefiles\trace.out
```

Spezielle Traceeinstellungen für den Journaldämon:

- BTREEDB - BTREE-Datenbankbasisklasse maschinennaher Ebene
- CACHEDB - Plattencachesicherung und Windows 2003-Cacheausschlussverarbeitung
- DBPERF - Leistung bei Datenbankoperation maschinennaher Ebene
- DBSTATS - Leistungsüberwachung bei Datenbankabfrage, Einfügen/Aktualisieren, Löschen und Walk-Operationen für Baumstruktur
- FILEOPS - interne Datenbankaktivität
- JBBCOMM - empfangsbereiter Thread
- JBBDAEMON - Prozessmanager
- JBBFILEMON - Dateisystemmonitor
- JBBDBACCESS - Datenbankcontroller-Thread
- JBBDBINFO - Datenbankzugriff maschinennaher Ebene
- JBBNPCOMM - Übertragung mit benannte Pipe
- JBBSERVICE - Windows-plattformspezifisches Service-Tracing
- JBBVERBINFO - ausführliche Verbinformationen
- ALL_JBB - zusammengefasstes Trace-Flag, das alle aufgeführten Einstellungen umfasst

Traceeinstellungen für den Client für Sichern/Archivieren, die in der Datei `dsm.opt` angegeben werden:

- JOURNAL - Tracing für journalbasierte Sicherung

Traceklassen für den Client

Der Client stellt einzelne und zusammengefasste Traceklassen bereit. Zusammengefasste Traceklassen sind ein Direktaufruf zur Aktivierung vieler verwandter Traceklassen. Dabei wird einfach der Name der zusammengefassten Traceklasse angegeben. Die dokumentierten Traceklassen können über Verweise auf Traceklassen verfügen, die als Teil einer zusammengefassten Traceklasse aktiviert, aber nicht separat erläutert werden.

Die in Tabelle 12 angegebenen Traceklassen sind die Traceklassen, die normalerweise angefordert oder für die Diagnose von Problemen verwendet werden. Der Traceklassenname muss mit den Optionen `TRACEFLAG` in der Datei `dsm.opt` verwendet werden.

Tabelle 12. Traceklassen

Traceklasse	Beschreibung	Empfehlung
ALL_BACK	Zeigt allgemeine Informationen zur Sicherungsverarbeitung für den Client an. Zusammenfassung der Traceklassen TXN, INCR, POLICY und PFM und implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse für Probleme, die sich auf selektive Sicherungen oder Teilsicherungen beziehen.
ALL_FILE	Zeigt allgemeine Informationen zur Sicherungsverarbeitung für den Client an. Zusammenfassung der Traceklassen DIROPS, FILEOPS und FIOATTRIBS und implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse für Probleme, die sich auf das Lesen und Schreiben von Daten sowie das Abrufen von Dateiattributdaten beziehen.
ALL_IMAGE	Zeigt Informationen zur Imageverarbeitung für den Client an. Zusammenfassung mehrerer imagebezogener Traceklassen und implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse für Probleme, die sich auf alle Aspekte der Datenträgerimagesicherungs- und -zurückschreibungsoperationen beziehen.
ALL_JBB	Zeigt Informationen zur journalbasierten Sicherungsverarbeitung für den Client an. Zusammenfassung mehrerer Traceklassen, die sich auf die journalbasierte Sicherung beziehen, und implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse für Probleme, die sich auf alle Aspekte der journalbasierten Sicherungen beziehen.
ALL_NAS	Zeigt Informationen zur NDMP-Verarbeitung für den Client an. Zusammenfassung mehrerer NDMP-bezogener Traceklassen und implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse für Probleme, die sich auf alle Aspekte der NDMP-Sicherungs- und -zurückschreibungsoperationen beziehen.

Tabelle 12. Traceklassen (Forts.)

Traceklasse	Beschreibung	Empfehlung
ALL_SESS	Zeigt alle Sitzungs- und Verbinformationen an, die zwischen dem Client und dem Server gesendet wurden. Zusammenfassung der Traceklassen SESSION, VERBINFO, SESSVERB, VERBADMIN und VERBDETAIL. Alle Traceklassen in dieser Zusammenfassung mit Ausnahme von VERBDETAIL sind implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse für Probleme, die sich auf die Client- und Serversitzung beziehen, wie z. B. Zeitlimitüberschreitung für Übertragung, fehlerhafte Protokolle und Situationen, in denen der Client gestoppt und auf den Server zu warten scheint, oder umgekehrt.
ALL_SNAPSHOT	Zeigt Informationen an, die sich auf Operationen mit Datenträgermomentaufnahmen beziehen. Zusammenfassung mehrerer Traceklassen, die sich auf Datenträgermomentaufnahmen beziehen, und implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse zur Bestimmung von Problemen bezüglich Datenträgermomentaufnahmen, die in Online-Imagesicherungen und Operationen für die Unterstützung offener Dateien verwendet werden.
ALL_WAS	Zeigt WAS-Verarbeitungsinformationen (WAS = Web Application Server) für den Client an. Zusammenfassung mehrerer WAS-bezogener Traceklassen und implizit in der Traceklasse SERVICE eingeschlossen.	Verwenden Sie diese Traceklasse für Probleme, die sich auf alle Aspekte der WAS-Sicherungs- und -zurückschreibungsoperationen beziehen.
AUDIT	Zeigt Prüfinformationen für die Sicherungs- und Zurückschreibungsverarbeitung an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um verarbeitete, festgeschriebene und zurückgeschriebene Dateien in einer Datei aufzuzeichnen.
CLIENTTYPE	Zeigt den Clienttyp in jeder Traceausgabezeile an.	Verwenden Sie diese Traceklasse, um einen Trace für Situationen zu erstellen, in denen mehrere Clientkomponenten betroffen sind, wie z. B. der Clientakzeptor und der Dateisystemagent.
COMPRESS	Zeigt Komprimierungsangaben an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um zu bestimmen, wie viele Daten pro Datei komprimiert werden.
DELTA	Zeigt Informationen zur Verarbeitung von adaptiven Subdateisicherungen an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um Fehler in adaptiven Subdateisicherungs- und -zurückschreibungsoperationen zu bestimmen.

Tabelle 12. Traceklassen (Forts.)

Traceklasse	Beschreibung	Empfehlung
DIROPS	Zeigt Lese- und Schreiboperationen für ein Verzeichnis an. Teil der Tracezusammenfassungen SERVICE und ALL_FILE.	Verwenden Sie diese Traceklasse, wenn Probleme beim Lesen oder Schreiben für ein Verzeichnis auftreten.
DOMAIN	Zeigt Informationen zur Verarbeitung von Teilsicherungen für Domänen an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um zu bestimmen, wie Anweisungen DOMAIN während der Sicherungsverarbeitung aufgelöst werden, wie z. B. bei Problemen mit der Auflösung der Domäne ALL-LOCAL.
ENCRYPT	Zeigt Informationen zur Datenverschlüsselung an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um zu bestimmen, ob eine Datei bei der Verschlüsselungsverarbeitung berücksichtigt wird.
ERROR	Zeigt betriebssystemspezifische Fehlerinformationen an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um Fehlercodes zu bestimmen, die vom Betriebssystem generiert wurden.
FILEOPS	Zeigt Lese- und Schreiboperationen für eine Datei an. Teil der Tracezusammenfassungen SERVICE und ALL_FILE.	Verwenden Sie diese Traceklasse, wenn Probleme beim Öffnen, Lesen, Schreiben oder Schließen einer Datei auftreten.
FIOATTRIBS	Zeigt Vergleiche von Dateiattributen zwischen der lokalen Clientversion und der aktiven Version auf dem Server an. Teil der Tracezusammenfassungen SERVICE, ALL_BACK und ALL_FILE.	Verwenden Sie diese Traceklasse, um zu bestimmen, warum eine Datei während einer Teilsicherung gesichert wurde.
INCR	Zeigt Vergleiche bei der Verarbeitung der Teilsicherungsliste zwischen dem Client und dem Server an. Teil der Tracezusammenfassungen SERVICE und ALL_BACK.	Verwenden Sie diese Traceklasse speziell in Verbindung mit der Traceklasse FIOATTRIBS, um zu bestimmen, ob Dateien Kandidaten für die Teilsicherung sind.
INCLEXCL	Zeigt den Einschluss/Ausschlussstatus für das Objekt an, das verarbeitet wird. Dieses Flag wird auch für die Voranzeigefunktion verwendet.	Verwenden Sie diese Traceklasse, um zu bestimmen, welches Objekt (normalerweise eine Datei oder ein Verzeichnis) bei der Sicherung, Archivierung oder Voranzeige eingeschlossen oder ausgeschlossen ist.
MEMORY	Zeigt Informationen zur Speicherzuordnung und zum freien Speicher an. Diese Traceklasse schreibt umfangreiche Informationen in die Tracedatei und ist in keiner zusammengefassten Klasse enthalten.	Verwenden Sie diese Traceklasse, um Speicherlecks, Speicherspitzen und andere speicherbezogene Probleme zu bestimmen.

Tabelle 12. Traceklassen (Forts.)

Traceklasse	Beschreibung	Empfehlung
OPTIONS	Zeigt aktuelle Verarbeitungsoptionen an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um die Optionen zu bestimmen, die für die aktuelle Sitzung wirksam sind, und Probleme beim Akzeptieren von Verarbeitungsoptionen aus Server-/Clientoptionsgruppen zu bestimmen.
PASSWORD	Zeigt Zugriffsinformationen für die Kennwortdatei an (zeigt keine Kennwörter an). Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um Probleme beim Lesen der Serverkennwörter aus dem lokalen Speicher zu bestimmen, z. B. Fehler bei PASSWORDACCESS=GENERATE.
PID	Zeigt die Prozess-ID in jeder Traceanweisung an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um Probleme zu diagnostizieren, die sich auf mehrere Prozesse beziehen können.
POLICY	Zeigt Maßnahmeninformationen an, die für den Client für Sichern/Archivieren verfügbar sind. Teil der Tracezusammenfassungen SERVICE und ALL_BACK.	Verwenden Sie diese Traceklasse, um die Maßnahmen zu bestimmen, die während einer Sicherungs- oder Archivierungsoperation verfügbar sind.
SCHEDULER	Zeigt allgemeine Verarbeitungsinformationen für den Scheduler an. Eine Zusammenfassung, die die meisten der in dieser Tabelle aufgelisteten Traceklassen für den Client enthält. Zusammenfassung aller Traceklassen, mit Ausnahme der Klassen MEMORY, THREAD_STATUS und *DETAIL.	In vielen Fällen nützlich. Diese Traceklasse wird für die Diagnose von Schedulerproblemen verwendet, wenn die genaue Ursache des Problems nicht bekannt ist. Wenn das Trace-Flag SCHEDULER verwendet wird, ist es im Allgemeinen nicht erforderlich, andere Trace-Flags anzugeben, da es bereits die meisten Basistraceklassen enthält.
SERVICE	Zeigt allgemeine Verarbeitungsinformationen für den Client an. Eine Zusammenfassung, die die meisten der in dieser Tabelle aufgelisteten Traceklassen für den Client enthält. Zusammenfassung aller Traceklassen, mit Ausnahme der Klassen MEMORY und *DETAIL. Das Trace-Flag SERVICE kann einen erheblichen Umfang an Informationen generieren. Ziehen Sie die Verwendung der Option TRACEMAX zusammen mit dem Trace-Flag SERVICE in Betracht.	In vielen Fällen nützlich. Diese Traceklasse wird verwendet, wenn die genaue Ursache des Problems nicht bekannt ist. Wenn das Trace-Flag SERVICE verwendet wird, ist es nicht erforderlich, andere Trace-Flags anzugeben, da es bereits die meisten Basistraceklassen enthält.

Tabelle 12. Traceklassen (Forts.)

Traceklasse	Beschreibung	Empfehlung
SESSION	Zeigt minimale Informationen zu Sitzungen zwischen dem Client und dem Server an. Teil der Tracezusammenfassungen SERVICE und ALL_SESS.	Verwenden Sie diese Traceklasse, um Sitzungskontext für allgemeine Verarbeitungsfehler bereitzustellen, oder verwenden Sie diese Traceklasse zusammen mit einer der Traceklassen VERB*, um Sitzungsprobleme, wie z. B. Sitzungszeitlimitüberschreitungen und fehlerhafte Protokolle, zu bestimmen.
SESSVERB	Zeigt zusätzliche Informationen zu Sitzungen zwischen dem Client und dem Server an. Teil der Tracezusammenfassungen SERVICE und ALL_SESS.	Verwenden Sie diese Traceklasse, um Sitzungskontext für allgemeine Verarbeitungsfehler bereitzustellen, oder verwenden Sie diese Traceklasse zusammen mit einer der Traceklassen VERB*, um Sitzungsprobleme, wie z. B. Sitzungszeitlimitüberschreitungen und fehlerhafte Protokolle, zu bestimmen.
STATS	Zeigt eine abschließende Verarbeitungsstatistik in der Tracedatei an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse, um eine abschließende Verarbeitungsstatistik in einer Datei zu erfassen.
THREAD_STATUS	Zeigt den Threadstatus an. Teil der Tracezusammenfassung SERVICE.	Verwenden Sie diese Traceklasse für die Diagnose von Problemen in Bezug auf Threading.
TXN	Zeigt Informationen zur Transaktionsverarbeitung an. Teil der Tracezusammenfassungen SERVICE und ALL_BACK.	Verwenden Sie diese Traceklasse für die Diagnose von Problemen in Bezug auf die Transaktionsverarbeitung auf dem Server und für die Diagnose von Problemen, wie Transaktionsstopps und -wiederholungen.
VERBDETAIL	Zeigt ausführliche Verbinformationen an, die für Client-/Serversitzungen relevant sind. Teil der Tracezusammenfassung ALL_SESS.	Verwenden Sie diese Traceklasse, um den Inhalt von Verben zu bestimmen, die zwischen dem Client und dem Server gesendet werden.
VERBINFO	Zeigt Verbinformationen an, die für Client-/Serversitzungen relevant sind. Teil der Tracezusammenfassungen SERVICE und ALL_SESS.	Verwenden Sie diese Traceklasse zusammen mit dem Trace-Flag SESSION, um Sitzungskontext für allgemeine Verarbeitungsfehler bereitzustellen oder Sitzungsprobleme, wie z. B. Sitzungszeitlimitüberschreitungen und fehlerhafte Protokolle, zu bestimmen.

Tabelle 12. Traceklassen (Forts.)

Traceklasse	Beschreibung	Empfehlung
WIN2K	Zeigt die Verarbeitung des Windows-Systemobjekts oder -Systemstatus an. Teil der Tracezusammenfassung SERVICE. Nur auf dem Windows-Client für Sichern/Archivieren gültig.	Verwenden Sie diese Traceklasse, um Fehler bei der Sicherung oder Zurückschreibung der Systemstatusinformationen zu bestimmen.

Trace für Client für Sichern/Archivieren aktivieren

Es gibt zwei Methoden für die Traceerstellung für den Client für Sichern/Archivieren.

Bei der ersten Methode werden Traceparameter konfiguriert, bevor der Client für Sichern/Archivieren gestartet wird. Bei der zweiten Methode wird das Tracing aktiviert, während der Client aktiv ist. Wählen Sie aus, welche Methode für die Traceerstellung aktiviert werden soll.

Client-Trace über die Befehlszeile aktivieren

Sie können einen Trace für den verfügbaren Client für Sichern/Archivieren durchführen, indem Sie den Client-Trace über die Befehlszeile aktivieren.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Client-Tracefunktion über die Befehlszeile zu aktivieren:

Vorgehensweise

1. Bestimmen Sie die Traceklassen, die aktiviert werden sollen.
2. Wählen Sie die zu aktivierenden Traceklassen aus, indem Sie der Clientoptionsdatei `dsm.opt` den folgenden Text hinzufügen: `traceflags <Name der Traceklasse>`.
3. Geben Sie vor einer Traceklasse ein Minuszeichen (-) an, um die Traceverarbeitung für eine Traceklasse zu inaktivieren. Stellen Sie sicher, dass die Traceklassen, deren Traceverarbeitung inaktiviert wurde, an das Ende der Traceklassenliste gestellt werden. Wenn Sie beispielsweise einen SERVICE-Trace ohne die Klassen SESSION und SESSVERB erfassen möchten, geben Sie den folgenden Text an:

   Korrekt: `traceflags service,-session,-sessverb`

   Falsch: `traceflags -session,-sessverb,service`

   Achtung: Bei *<Name der Traceklasse>* kann es sich um eine Liste mit durch Kommas getrennten Traceklassen handeln. Es kann beispielsweise Folgendes angegeben werden: `traceflags service,verbdetail`.
4. Wählen Sie die Speicherposition für die Ausgabe der Tracenachrichten aus, indem Sie der Clientoptionsdatei den folgenden Text hinzufügen: `tracefile <Dateiname>`.

   Der Name der *Tracedatei* muss ein vollständig qualifizierter Name sein, wie beispielsweise:

   Windows `tracefile c:\service\trace.out`

   AIX Linux `tracefile /home/spike/trace.out`

Mac OS X `tracefile trace.txt`

5. Definieren Sie eine maximale Größe von 1 bis 4.294.967.295 MB für die Tracedatei, indem Sie die folgende Variable in der Clientoptionsdatei angeben: `tracemax <Größe in MB>`.

   Wenn ein Maximalwert angegeben wird, beginnt der Client, die Informationen am Anfang der Tracedatei zu überschreiben (Umlauf), wenn die maximale Größe der Tracedatei erreicht ist. Dies kann hilfreich sein, wenn versucht wird, ein Ereignis zu erfassen, das am Ende eines Prozesses mit langer Laufzeit stattfindet. Beispiel: Um eine maximale Tracedateigröße von 10 MB festzulegen, geben Sie `tracemax 10` an. Nachdem eine Tracedatei den durch tracemax angegebenen Grenzwert erreicht hat, wird „Wird am Dateianfang fortgesetzt" am Ende der Tracedatei ausgegeben und die Tracefunktion am Anfang der Datei fortgesetzt. Das Ende der Tracedatei wird durch „DATENENDE" angegeben. Sie können das Ende des Trace lokalisieren, indem Sie nach dieser Zeichenfolge suchen. Wenn Sie mit TRACEMAX eine Größe von 1001 oder mehr angeben und TRACESEGSIZE nicht angegeben wird, wird die Tracedatei automatisch in mehrere Segmente von je 1000 MB aufgeteilt (siehe die Informationen zu TRACESEGSIZE).

   Falls gewünscht, können Sie den Trace vom Client in kleinere Segmente (1 - 1.000 MB pro Segment) aufteilen lassen, indem Sie in der Clientoptionsdatei die folgende Variable angeben: `tracesegsize <Tracesegmentgröße in MB>`.

   Die Aufteilung des Trace in kleinere Segmente erleichtert Ihnen die Verwaltung großer Volumen an Tracedaten, da die Probleme, die mit dem Komprimieren großer Dateien verbunden sind, verhindert werden und die Notwendigkeit zur Verwendung eines separaten Dienstprogramms „file splitter" eliminiert wird. Geben Sie beispielsweise den folgenden Befehl aus, um eine Tracesegmentgröße von 200 MB anzugeben: `tracesegsize 200`.

   Ein Tracedateisegmentname wird mit der Option tracefile zusammen mit einer Erweiterung angegeben, die die Segmentnummer angibt. Wenn Sie beispielsweise `tracefile tsmtrace.out` und `tracesegsize 200` angeben, wird der Trace in mehrere separate Dateien segmentiert, von denen jede nicht größer als 200 MB ist und deren Dateinamen wie folgt lauten: `tsmtrace.out.1`, `tsmtrace.out.2` usw. Bei der Angabe der Segmentgröße dürfen keine Kommatrennzeichen verwendet werden:

   Korrekt: `tracemax 1000`

   Falsch: `tracemax 1,000`

   Wenn Sie die Option `TRACESEGSIZE` verwenden, werden die Tracedateisegmente unter Verwendung des in der Optionsdatei angegebenen Namens benannt, wobei die Segmentnummer als zusätzliche Erweiterung hinzugefügt wird. Beispiel: `trace.out.1`.

6. Führen Sie die Operation aus, bei der das Problem auftritt.

Nächste Schritte

Die Tracefunktion kann auch konfiguriert und gestartet werden, indem der Client über eine Eingabeaufforderung unter Angabe der zuvor definierten Flags gestartet wird. Beispiel:

```
dsmc -traceflags=service,verbdetail -tracefile=tsmtrace.out
-tracemax=2500 -tracesegsize=200
```

Zugehörige Verweise:

„Traceklassen für den Client" auf Seite 156

Trace während der Ausführung des Clients aktivieren

Sie können einen Trace für den verfügbaren Client für Sichern/Archivieren durchführen, während der Client aktiv ist.

Vorbereitende Schritte

- Der Client für Sichern/Archivieren muss für die Verwendung der dynamischen Tracefunktion installiert sein.
- Die Option `DSMTRACELISTEN YES` muss wirksam sein, wenn der Client gestartet wird.
  - AIX Linux Diese Option wird in der Systemoptionsdatei (`dsm.sys`) in der Zeilengruppe angegeben, die vom Client verwendet wird. Benutzer müssen als Root angemeldet sein, um dsmtrace verwenden zu können.
  - Windows Diese Option wird in der Clientoptionsdatei angegeben (normalerweise `dsm.opt`). Benutzer müssen als Mitglied der Gruppe 'Administratoren' angemeldet sein.

Wenn der Client gestartet wird, startet er einen separaten Thread „trace listener". Dieser Thread ist an einer benannten Pipe empfangsbereit und wartet darauf, vom Dienstprogramm dsmtrace kontaktiert zu werden. Da der Name der benannten Pipe eindeutig sein muss, ist die Prozess-ID (PID) des Clients Teil des Pipenamens. Wenn Sie dsmtrace zum Konfigurieren der Tracefunktion verwenden, kontaktiert dsmtrace den Client über die benannte Pipe, an der der Client empfangsbereit ist, und übergibt die bevorzugte Tracekonfigurationsoperation an den Client. Der Client gibt dann die Ergebnisse der Operation über eine andere ähnlich benannte Ausgabepipe an dsmtrace zurück. Die Ergebnisse werden von dsmtrace an der Konsole angezeigt. Der Client startet den Thread 'trace listener' nur, wenn die Clientoption `DSMTRACELISTEN YES` wirksam ist. Wenn `DSMTRACELISTEN NO` wirksam ist, wird der Listener-Thread nicht gestartet und die dynamische Tracefunktion ist für diesen Client nicht verfügbar. Der Standardwert ist `DSMTRACELISTEN NO`.

Informationen zu diesem Vorgang

Die Schritte zum Zusammenstellen eines Client-Trace sind wie folgt:

Vorgehensweise

1. Stoppen Sie den Client für Sichern/Archivieren.
2. Konfigurieren Sie die Clientoptionsdatei mit den bevorzugten Traceoptionen.
3. Starten Sie den Client für Sichern/Archivieren erneut und reproduzieren Sie das Problem.
4. Stoppen Sie den Client für Sichern/Archivieren.
5. Entfernen Sie die Traceoptionen aus der Optionsdatei des Clients für Sichern/Archivieren.
6. Senden Sie die resultierende Tracedatei zur Analyse an die technische Unterstützung von IBM.

   Sie können auch das Dienstprogramm dsmtrace verwenden, um die Client-Tracefunktion dynamisch zu starten, zu stoppen und zu konfigurieren, ohne den Client stoppen oder die Optionsdatei ändern zu müssen. Die dynamische Tracefunktion ist besonders nützlich, wenn Sie nur für den Anfang einer Operation des Clients für Sichern/Archivieren mit langer Laufzeit einen Trace durchführen müssen oder wenn Sie die Tracefunktion starten müssen, nachdem der Client für Sichern/Archivieren bereits einige Zeit aktiv ist.

   Das Dienstprogramm dsmtrace umfasst die folgenden Funktionen:

- Identifizieren aktiver Prozesse und ihrer Prozess-IDs (PIDs)
- Aktivieren der Client-Tracefunktion
- Inaktivieren der Client-Tracefunktion
- Abfragen des Client-Trace-Status

In der folgenden Tabelle ist die Verfügbarkeit dieses Dienstprogramms zusammengefasst:

Tabelle 13. Verfügbarkeit des Dienstprogramms dsmtrace

Clientkomponente	Name des AIX- oder Linux-Programms	Name des Windows-Programms
Client für Sichern/Archivieren (Befehlszeile)	dsmc	`dsmc.exe`
Client für Sichern/Archivieren (GUI)	Nicht zutreffend	`dsmagent.exe`
Clientakzeptor	dsmcad	`dsmcad.exe`
Ferner Clientagent	dsmagent	`dsmagent.exe`
Scheduler-Service	Nicht zutreffend	`dsmcsvc.exe`
Journalservice	Nicht zutreffend	`tsmjbbd.exe`
Data Protection for Domino (Befehlszeile)	domdsmc	`domdsmc.exe`
Data Protection for Domino (GUI)	Nicht zutreffend	`domdsm.exe`
Data Protection for Microsoft Exchange (Befehlszeile)	Nicht zutreffend	`tdpexcc.exe`
Data Protection for Microsoft Exchange (GUI)	Nicht zutreffend	`tdpexc.exe`
Data Protection for Microsoft SQL Server (Befehlszeile)	Nicht zutreffend	`tdpsqlc.exe`
Data Protection for Microsoft SQL Server (GUI)	Nicht zutreffend	`tdpsql.exe`

Anmerkung:

- Die mittlere Spalte in Tabelle 13 umfasst Macintosh OS X.
- Die Tracefunktion für die Data Protection-Komponenten gilt nur für die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API).
- Die IBM Spectrum Protect-API-Tracefunktion ist über jede Multithread-Anwendung verfügbar, die die IBM Spectrum Protect-API verwendet. Der Name der ausführbaren Datei ist der Name des Anwendungsprogramms, das die API lädt.

Beispiel

In dem folgenden Beispiel wird gezeigt, wie Sie den Client-Trace aktivieren können, während der Client aktiv ist:

1. Identifizieren Sie die Prozess-ID (PID) des Clients für Sichern/Archivieren, für den ein Trace durchgeführt werden soll (stellen Sie sicher, dass die Option `DSMTRACELISTEN YES` wirksam ist). Geben Sie den folgenden Befehl aus, um alle aktiven Instanzen des Clients anzuzeigen: `dsmtrace query pids`.

   Beispielausgabe:

```
D:\tsm>dsmtrace query pids

IBM Spectrum Protect
Dienstprogramm dsmtrace
 dsmtrace - Version 5, Release 3, Level 0.0
  dsmtrace - Datum/Uhrzeit: 10/24/2004 21:07:36
(c) Copyright IBM Corporation und andere 1990, 2004. Alle Rechte vorbehalten.

PROZESS-ID  PROZESSEIGNER  BESCHREIBUNG        NAME DER AUSFÜHRBAREN DATEI
4020        Andy           Client für Sichern/ dsmc.exe
                           Archivieren (CLI)
D:\tsm>
```

Wichtig: Linux Gemäß dem Threading-Modell für einige Versionen von Linux wird jeder Thread als separater Prozess ausgeführt. Dies bedeutet, dass beim Abfragen von Prozessinformationen möglicherweise mehrere Prozesse für jede Instanz des Clients angezeigt werden. Bei dem Prozess, den Sie identifizieren müssen, handelt es sich um den übergeordneten dsmc-Prozess. Beispiel:

```
fvtlinuxppc:/opt/tivoli/tsm/client/ba/bin # dsmtrace q p

IBM Spectrum Protect
Dienstprogramm dsmtrace
 dsmtrace - Version 5, Release 3, Level 0.0
  dsmtrace - Datum/Uhrzeit: 10/24/04 08:07:37
(c) Copyright IBM Corporation und andere 1990, 2004. Alle Rechte vorbehalten.

PROZESS-ID  PROZESSEIGNER  BESCHREIBUNG                        NAME DER
                                                               AUSFÜHRBAREN DATEI
28970       Root           Client für Sichern/Archivieren (CLI) dsmc
28969       Root           Client für Sichern/Archivieren (CLI) dsmc
28968       Root           Client für Sichern/Archivieren (CLI) dsmc
28967       Root           Client für Sichern/Archivieren (CLI) dsmc

fvtlinuxppc:/opt/tivoli/tsm/client/ba/bin #
```

Geben Sie in einer derartigen Situation den Befehl **PS** aus, um den übergeordneten dsmc-Prozess zu identifizieren:

```
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:~ #
```

Beachten Sie, dass der Prozess 28968 der übergeordnete Prozess für die Prozesse 28969 und 28970 ist. Der übergeordnete Prozess für 28968 ist der Prozess 28967. Der übergeordnete Prozess für 28967 ist der Prozess 1151, der Prozess 1151 wird jedoch in dieser Bildschirmausgabe nicht angezeigt. Prozess 1151 ist der Prozess, mit dem dsmc gestartet wurde. Demzufolge ist die korrekte übergeordnete Prozess-ID 28967.

2. Geben Sie den folgenden Befehl aus, um die Tracefunktion auf dem Client zu aktivieren:

   ```
   dsmtrace enable 4020 -traceflags=service -tracefile=d:\trace.txt
   ```

   Beispielausgabe:

   ```
   C:\Programme\tivoli\tsm\baclient>dsmtrace enable 4020 -traceflags=service
   -tracefile=d:\trace.txt

   IBM Spectrum Protect
   ```

```
Dienstprogramm dsmtrace
 dsmtrace - Version 5, Release 3, Level 0.0
  dsmtrace - Datum/Uhrzeit: 10/24/2004 21:45:54
(c) Copyright IBM Corporation und andere 1990, 2004. Alle Rechte vorbehalten.

ANS2805I Ablaufverfolgung wurde aktiviert.

C:\Programme\tivoli\tsm\baclient>
C:\Programme\tivoli\tsm\baclient>
```

Wichtig: Wenn Sie einen Trace für eine API-Anwendung durchführen, muss die Option `-pipenameprefix` eingeschlossen werden.

- AIX Linux Verwenden Sie das Präfix `/tmp/TsmTraceTargetAPI`.
- Windows Verwenden Sie das Präfix `\\.\pipe\TsmTraceTargetAPI`.

3. Nachdem genügend Tracedaten erfasst wurden, inaktivieren Sie die Tracefunktion, indem Sie den folgenden Befehl ausgeben:

   ```
   dsmtrace disable 4020
   ```

   Beispielausgabe:

   ```
   C:\Programme\tivoli\tsm\baclient>dsmtrace disable 4020

   IBM Spectrum Protect
   Dienstprogramm dsmtrace
     dsmtrace - Version 5, Release 3, Level 0.0
     dsmtrace - Datum/Uhrzeit: 10/24/2004 21:47:43
   (c) Copyright IBM Corporation und andere 1990, 2004. Alle Rechte vorbehalten.

   ANS2802I Ablaufverfolgung wurde inaktiviert.
   ```

Weitere Beispiele für die Aktivierung des Client-Trace, während der Client aktiv ist, sind in der folgenden Liste definiert:

dsmtrace query pids
: Mit diesem Befehl werden alle aktiven Prozesse angezeigt, deren Namen in der Tabelle im Abschnitt mit den Hintergrundprozessen aufgelistet sind.

dsmtrace query pids -filter=*
: Mit diesem Befehl werden alle aktiven Prozesse angezeigt.

dsmtrace query pids -filter=dsm*
: Mit diesem Befehl werden alle aktiven Prozesse angezeigt, deren Namen mit „dsm" beginnen.

dsmtrace query pids -filter=dsm?
: Mit diesem Befehl werden alle aktiven Prozesse angezeigt, deren Namen mit „dsm" sowie einem weiteren Zeichen beginnen.

dsmtrace enable 2132 -traceflags=service -tracefile=c:\trace.txt
: Mit diesem Befehl wird die SERVICE-Tracefunktion für Prozess 2132 aktiviert. Die Traceausgabe wird in die Datei `c:\trace.txt` geschrieben.

dsmtrace enable 2132 -traceflags=-extrc
: Mit diesem Befehl wird die Tracefunktion für Prozess 2132 inaktiviert (vorausgesetzt, die Tracefunktion für diesen Prozess ist bereits aktiv).

dsmtrace enable 4978 -traceflags=fileops -tracefile=/tmp/dsmtrace.out -tracemax=1000 -tracesegsize=200
: Mit diesem Befehl wird die FILEOPS-Tracefunktion für Prozess 4978 aktiviert. Der Trace wird in die Dateien `/tmp/dsmtrace.out.1`, `/tmp/dsmtrace.out.2` usw. geschrieben; dabei hat jede Datei eine maximale

Größe von 200 MB. Nachdem 1000 MB ausgegeben wurden, erfolgt für die Tracefunktion ein Umlauf zurück zu Datei `/tmp/dsmtrace.out.1`.

`dsmtrace query trace 4978 -on`
Mit diesem Befehl werden grundlegende Traceinformationen angezeigt und Trace-Flags aufgelistet, die für Prozess 4978 aktiviert sind.

`dsmtrace disable 4978`
Mit diesem Befehl wird die Tracefunktion für Prozess 4978 inaktiviert.

`dsmtrace disable 364 -pipenameprefix=/tmp/TsmTraceTargetAPI`
Mit diesem Befehl wird die Tracefunktion für den API-Anwendungsprozess 364 inaktiviert.

Bekannte Probleme und Einschränkungen für die Traceerstellung

Die bekannten Probleme und Einschränkungen für Traceprozesse werden zusammengestellt, um Ihnen bei der Behebung von Problemen zu helfen, die möglicherweise bei der Ausführung eines Traceprozesses festgestellt werden.

- Wenn die Tracefunktion für einen Prozess gegenwärtig nicht aktiv ist und 'dsmtrace' nur mit der Option `-TRACEFLAGS` verwendet wird (z. B. **`dsmtrace enable 2346 -traceflags=service`**), wird dennoch die folgende Nachricht angezeigt:

  ```
  ANS2805I Ablaufverfolgung wurde aktiviert.
  ```

  In diesem Fall wurden die Trace-Flags aktiviert, aber die Tracefunktion ist erst dann aktiv, wenn eine Tracedatei mit der Option -TRACEFILE angegeben wird.
- Verwenden Sie nicht den Befehl 'dsmtrace enable' zum Starten der Traceerstellung für die Anwendungsprogrammierschnittstelle (API) für Data Protection-Anwendungen, wenn die Data Protection-Anwendung in einer Art und Weise ausgeführt wird, in der keine Verbindung zum IBM Spectrum Protect-Server hergestellt wird. Beispielsweise hat die Data Protection for IBM Domino-Befehlszeilenschnittstelle mehrere der folgenden Befehle:
  - domdsmc help
  - domdsmc set
  - domdsmc query domino
  - domdsmc query pendingdbs
  - domdsmc query preferences

  Wenn Sie 'dsmtrace' verwenden, um die Tracefunktion für diese Befehle zu aktivieren, können ein Stopp des dsmtrace-Prozesses und (nur für AIX und Linux) der Verbleib eines Rests einer benannten Pipe im Verzeichnis /tmp die Folge sein.
- Windows Sie müssen sich mit einem lokalen Verwaltungsaccount anmelden, um 'dsmtrace' zu verwenden.
- Sie müssen sich als Root anmelden, um 'dsmtrace' zu verwenden. Wenn ein Clientprozess stoppt oder gestoppt wird, kann eine benannte Pipe (UNIX FIFO) im Verzeichnis /tmp verbleiben. Diese FIFOs haben Namen, die mit 'TsmTrace' beginnen, und schließen eine Prozess-ID (PID) ein. Wenn ein Clientprozess stoppt oder gestoppt wird und dann ein neuer Clientprozess gestartet wird, dessen PID mit der PID der alten verbliebenen FIFO übereinstimmt, wird der Thread 'trace listener' möglicherweise nicht gestartet. Alle alten FIFOs mit Prozessnummern, die nicht mit den FIFOs der aktiven IBM Spectrum Protect-Prozesse übereinstimmen, können gelöscht werden. Löschen Sie NICHT die FIFO eines aktiven Prozesses.
- Gemäß dem Threading-Modell für einige Versionen von Linux wird jeder Thread als separater Prozess ausgeführt. Dies bedeutet, dass beim Abfragen von Prozessinformationen möglicherweise mehrere Prozesse für jede Instanz des Cli-

ents angezeigt werden. Bei dem Prozess, den Sie identifizieren müssen, handelt es sich um den übergeordneten dsmc-Prozess.

- Wenn mehrere Instanzen desselben Programms ausgeführt werden, müssen Sie die PID der Instanz identifizieren, für die ein Trace durchgeführt werden soll. In einer solchen Situation sind möglicherweise Informationen wie beispielsweise die Prozessinformationen aus dem Betriebssystem verfügbar, mit deren Hilfe Sie die erforderliche PID ermitteln können. Wenn beispielsweise ein Trace für das Programm 'dsmc' durchgeführt werden soll, das vom Benutzer 'andy' ausgeführt wird, und zwei Instanzen von 'dsmc' vorhanden sind (der Eigner einer Instanz ist der Benutzer 'andy' und der Eigner der anderen Instanz ist der Benutzer 'kevin'), können Sie den Prozesseigner verwenden, um den Prozess anzugeben, für den ein Trace durchgeführt werden soll.
- Wenn eine Optionsdatei eine falsche Option enthält und der Client nicht gestartet wird, werden möglicherweise einige Fehler zur benannten Pipe in der Datei `dsmerror.log` angezeigt. Diese Fehlernachrichten können beruhigt ignoriert werden.

Traceoptionen

Die Tracefunktion hat verschiedene Optionen, die Sie verwenden können.

DSMTRACEListen

DSMTRACEListen No | Yes

No Der Client startet nicht den Thread 'trace listener' und die dynamische Tracefunktion ist nicht verfügbar. Der Standardwert ist No.

Yes Der Client startet den Thread 'trace listener' und die dynamische Tracefunktion ist verfügbar.

Windows Die Option `DSMTRACEListen` wird in der Clientoptionsdatei angegeben (normalerweise `dsm.opt`).

dsmtrace

dsmtrace enable <*PID*> <*Optionen*>

Verwenden Sie diesen Befehl, um die Traceerstellung für einen Prozess zu starten oder zu ändern.

PID Die Prozess-ID (PID) für den Client. Verwenden Sie 'dsmtrace query pids' oder die Betriebssystemfunktionen, um die korrekte PID anzugeben.

Optionen
Die Client-Traceoptionen.

dsmtrace disable <*PID*>[<*Optionen*>]

Verwenden Sie diesen Befehl, um die Traceerstellung für einen Prozess zu stoppen. Die Tracedatei wird geschlossen und die Trace-Flags, die maximale Tracegröße, die maximale Tracesegmentgröße und der Tracedateiname werden gelöscht.

<*PID*> Die PID für den Client. Verwenden Sie **dsmtrace query pids** oder die Betriebssystemfunktionen, um die korrekte PID anzugeben.

<*Optionen*>
Die Client-Traceoptionen.

dsmtrace help

Dieser Befehl zeigt grundlegende Syntax für 'dsmtrace' an.

dsmtrace query pids [-Filter=<*Spezifikation*>]

<Spezifikation>
Die Namensfilterspezifikation für den Clientprozess, die das Platzhalterzeichen „?" (entspricht exakt einem Zeichen) oder „*" (entspricht null oder mehr Zeichen) enthalten kann.

Wird kein Filter angegeben, werden standardmäßig Prozessinformationen für alle aktiven Instanzen der Programme angezeigt, die in der Tabelle im Abschnitt mit den Hintergrundprozessen oben aufgelistet sind.

Wichtig: AIX Linux Wenn Sie FILTER verwenden, setzen Sie das Symbol * vor und hinter den Suchbegriff. Diese Anpassung ist erforderlich, weil vor dem Namen der ausführbaren Datei oft der Pfad steht und in manchen Fällen zusätzliche Zeichen am Ende des Namens der ausführbaren Datei stehen. Beispiel:

- `/opt/tivoli/tsm/client/ba/bin/dsmc`
- `domdsmc_DominoUserID`

Statt -filter=dsmc oder -filter=domdsmc müssen Sie daher -filter=*dsmc* oder -filter=*domdsmc* verwenden.

dsmtrace query trace <*PID*> [<*Optionen*>] [<*Anzeigetyp*>] [-ALl | -ON | -OFf | -BASic]

<*PID*> Die Prozess-ID (PID) für den Client. Verwenden Sie 'dsmtrace query pids' oder die Betriebssystemfunktionen, um die korrekte PID anzugeben.

<Optionen>
Die Client-Traceoptionen.

<Anzeigetyp>
Der Anzeigetyp kann einer der folgenden Einträge sein:

ALl Zeigt alle Trace-Flags an und gibt für jedes Flag an, ob es aktiviert oder inaktiviert ist. Die mit dem Anzeigetyp -BASIC angezeigten Informationen sind ebenfalls eingeschlossen.

ON Zeigt die Namen der Trace-Flags an, die aktiviert sind. Die mit dem Anzeigetyp -BASIC angezeigten Informationen sind ebenfalls eingeschlossen.

OFf Zeigt die Namen der Trace-Flags an, die inaktiviert sind. Die mit dem Anzeigetyp -BASIC angezeigten Informationen sind ebenfalls eingeschlossen.

BASic Zeigt den Namen der Tracedatei und die maximalen Trace- und Tracesegmentgrößen an. Dieser Anzeigetyp gibt auch an, ob die Tracefunktion aktiviert oder inaktiviert ist.

`-PIPENameprefix`

`-PIPENameprefix`=<*Pipenamenspräfix*>
Die Option `-PIPENameprefix` muss verwendet werden, wenn ein Trace für API-Anwendungen durchgeführt wird:

- AIX Linux Verwenden Sie das Präfix `/tmp/TsmTraceTargetAPI`.
- Windows Verwenden Sie das Präfix `\\.\pipe\TsmTraceTargetAPI`.

-TRACEFIle

-TRACEFIle=<*Tracedateiname*>
Die Option -TRACEFIle muss einen gültigen Namen für eine Datei angeben, in die der Trace geschrieben wird. Wird die Tracefunktion bereits ausgeführt, hat diese Option keine Auswirkungen.

-TRACEFLags

-TRACEFLags=<*Trace-Flags*>
Geben Sie ein oder mehrere Trace-Flags an. Normalerweise wird das Trace-Flag SERVICE verwendet. Trennen Sie mehrere Trace-Flags durch ein Komma. Trace-Flags können auch inaktiviert werden, indem dem Namen des Flags ein Minuszeichen vorangestellt wird. Wenn Trace-Flags, die aktiviert werden sollen, mit Trace-Flags kombiniert werden, die inaktiviert werden sollen, stellen Sie die Flags, die inaktiviert werden sollen, an das Ende der Liste. Wenn Sie beispielsweise die SERVICE-Tracefunktion außer für VERBDETAIL aktivieren möchten, geben Sie -TRACEFLAGS=SERVICE,-VERBDETAIL an. Wird die Tracefunktion bereits ausgeführt, kann diese Option verwendet werden, um weitere Trace-Flags zu aktivieren oder Trace-Flags zu inaktivieren.

-TRACEMax

-TRACEMax=<*maximale Tracegröße*>
Mit dieser Option wird die maximale Länge der Tracedatei auf den angegebenen Wert begrenzt (standardmäßig nimmt die Größe der Tracedatei unbegrenzt zu). Wenn die maximale Länge erreicht ist, beginnt die Traceerfassung wieder am Anfang der Datei. Geben Sie einen Wert in MB zwischen 1 und 4095 an. Wird die Tracefunktion bereits ausgeführt, hat diese Option keine Auswirkungen.

-TRACESegsize

-TRACESegsize=<*maximale Tracesegmentgröße*>
Diese Option wird verwendet, wenn eine große Tracedatei erwartet wird und die Tracedatei in kleinere, einfacher zu verwaltende Segmente geschrieben werden soll. Kein Segment überschreitet die angegebene Größe. Bei Verwendung dieser Option wird eine Segmentnummer an den Namen der Tracedatei für jedes Segment angehängt. Geben Sie einen Wert in MB zwischen 1 und 1000 an. Wird die Tracefunktion bereits ausgeführt, hat diese Option keine Auswirkungen.

Anmerkung:

- Um die Tracefunktion für einen Prozess zu aktivieren, müssen Sie die Optionen -TRACEFLAGS und -TRACEFILE verwenden (und -PIPENAMEPREFIX, wenn ein Trace für eine API-Anwendung durchgeführt wird).
- Um Trace-Flags für einen vorhandenen Prozess zu ändern, verwenden Sie -TRACEFLAGS (und -PIPENAMEPREFIX, wenn ein Trace für eine API-Anwendung durchgeführt wird).
- Wenn Sie den Tracedateinamen, die maximale Tracegröße oder die maximale Tracesegmentgröße ändern müssen, müssen Sie zuerst die gesamte Tracefunktion inaktivieren (siehe Befehl **dsmtrace disable**).

Mithilfe eines Trace bestimmen, ob Daten während der Sicherung/Archivierung verschlüsselt oder komprimiert sind

Sie müssen verschiedene Schritte ausführen, um bestimmen zu können, ob Daten während der Sicherung/Archivierung komprimiert und/oder verschlüsselt sind.

Vorgehensweise

1. Fügen Sie der Clientoptionsdatei die aufgelisteten Traceoptionen hinzu, bevor Sie Objekte sichern oder archivieren:
   - TRACEFILE <*Tracedateiname*>
   - TRACEFLAGS api api_detail
2. Überprüfen Sie die Tracedatei nach der Operation und suchen Sie eine Anweisung, die ähnlich wie die folgende aussieht:

   dsmSendObj ENTRY:... objNameP: <*Dateiname*>

   Auf diese Ausgabe folgt die folgende Tracenachricht, die angibt, ob das Objekt komprimiert und/oder verschlüsselt ist:

   ```
   tsmEndSendObjEx: Total bytes send * *, encryptType is *** encryptAlg is ***
   compress is *, totalCompress is * * totalLFBytesSent * *
   ```

   ```
   +-------------------------------------------------------------------+
   | encryptType/compress | 0 | 1 |
   +-------------------------------------------------------------------+
   | NO | not compressed, not encrypted | compressed, not encrypted |
   | CLIENTENCRKEY | not compressed, encrypted | compressed, encrypted |
   | USER | not compressed, encrypted | compressed, encrypted |
   +-------------------------------------------------------------------+
   ```

   Stattdessen kann Ihre Anwendung über den Funktionsaufruf **dsmEndSendObjEx** und die Datenstruktur **dsmEndSendObjExOut_t** selbst den Verschlüsselungstyp/die Verschlüsselungsstufe und die Komprimierung Ihrer Daten bestimmen.

   ```
   /*-------------------------------------------------------------------+
   | Typdefinition für dsmEndSendObjExOut_t
   +-------------------------------------------------------------------*/
   typedef struct dsmEndSendObjExOut_t
   {
   dsUint16_t     stVersion;          /* Strukturversion */
   dsStruct64_t   totalBytesSent;     /* Gesamtsumme aus Anwendung gelesener Byte */
   dsmBool_t      objCompressed;      /* mit Objektkomprimierung */
   dsStruct64_t   totalCompressSize;  /* Gesamtgröße nach Komprimierung */
   dsStruct64_t   totalLFBytesSent;   /* Gesamtanzahl LAN-unabhängig gesendeter Byte */
   dsUint8_t      encryptionType;     /* verwendeter Verschlüsselungstyp */
   }dsmEndSendObjExOut_t;

   objCompressed  - Ein Flag, das angezeigt wird, wenn das Objekt komprimiert war.
   encryptionType - Ein Flag, das den Verschlüsselungstyp anzeigt.

   Beispiel:

     ...
     rc = dsmEndSendObjEx(&endSendObjExIn, &endSendObjExOut);
     if (rc)
     {
     printf("*** dsmEndSendObjEx fehlgeschlagen: ");
     rcApiOut(dsmHandle, rc);
   }
   else
   {
    printf("Komprimierung: %s\n",
    endSendObjExOut.objCompressed == bTrue ? "YES" : "NO");

    printf("Verschlüsselung: %s\n",
   ```

```
endSendObjExOut.encryptionType & DSM_ENCRYPT_CLIENTENCRKEY ?
"CLIENTENCRKEY" :
endSendObjExOut.encryptionType & DSM_ENCRYPT_USER ? "USER" : "NO");
printf("Verschlüsselungsstufe: %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");
}
...
```

Nächste Schritte

Weitere Informationen finden Sie unter *API-Funktionsaufrufe* im Handbuch *Verwendung der Anwendungsprogrammierschnittstelle*.

Trace für API-Daten durchführen

Sie können die Tracefunktion für die Anwendungsprogrammierschnittstelle (API) aktivieren.

Um die Tracefunktion für die IBM Spectrum Protect-API zu aktivieren, fügen Sie die folgenden Zeilen zur Datei `dsm.opt` oder zu einer anderen Datei hinzu, die als Clientoptionsdatei angegeben ist:

```
TRACEFILE Tracedateiname
TRACEFLAGS Trace-Flags
```

Tracedateiname
Der Name der Datei, in die die Tracedaten geschrieben werden sollen.

Trace-Flags
Die Liste der Trace-Flags, die aktiviert werden sollen. Trennen Sie jedes Trace-Flag durch ein Leerzeichen. Die folgenden Trace-Flags gelten speziell für die IBM Spectrum Protect-API:

api Informationen zu den API-Funktionsaufrufen

api_detail
Ausführliche Informationen zu den API-Funktionsaufrufen

Sie können auch andere Trace-Flags für den Client für Sichern/Archivieren und die IBM Spectrum Protect-API angeben. Eine Liste der verfügbaren Traceklassen befindet sich in der Dokumentation für den Client für Sichern/Archivieren. Beispiel:

- `TRACEFILE /log/trace.out`
- TRACEFLAGS api api_detail verbinfo verbdetail time stamp

Wichtig: Wenn Sie keine Schreibberechtigung für die Datei haben, auf die durch die Option TRACEFILE verwiesen wird, schlägt 'dsmSetup' oder 'dsmInitEx/ dsmInit' mit dem Rückkehrcode DSM_RC_CANNOT_OPEN_TRACEFILE (426) fehl.

Um die Tracefunktion für die Multithread-API nach dem Start einer Anwendung zu aktivieren, verwenden Sie das Dienstprogramm `dsmtrace`. Mit dem Dienstprogramm `dsmtrace` können Sie die Tracefunktion aktivieren, wenn das Problem auftritt, ohne dass die Tracefunktion ständig aktiviert sein muss. Lesen Sie den Abschnitt *dsmtrace*.

Trace für den Tivoli Monitoring for Tivoli Storage Manager-Agenten auf einem AIX- oder Linux-System durchführen

AIX Linux

Mithilfe von Tivoli Monitoring for Tivoli Storage Manager können Sie Agenteninstanzen, die IBM Spectrum Protect-Server überwachen, erstellen und konfigurieren. Um die Tracefunktion für die Überwachungsagenten für Server, die auf AIX- oder Linux-Systemen ausgeführt werden, zu aktivieren, stoppen Sie alle Agenteninstanzen, ändern Sie die Konfigurationsdateien und starten Sie die Agenteninstanzen erneut.

Informationen zu diesem Vorgang

Bevor Sie die Tracefunktion aktivieren, können Sie auch den Tivoli Enterprise Portal-Arbeitsbereich 'Agentenprotokoll' öffnen und die Agentenaktivitäten anzeigen. Der Arbeitsbereich 'Agentenprotokoll' enthält Informationen zu jedem IBM Spectrum Protect-Server, für den eine Agenteninstanz zur Überwachung des Servers konfiguriert ist. Mithilfe der Attributgruppe 'Agentenprotokoll' können Sie die Ausgabe der Tracedatei anzeigen, ohne die Tracedatei zu aktivieren.

Führen Sie die folgenden Schritte aus, um die Tracefunktion zu aktivieren:

Vorgehensweise

1. Wechseln Sie in einer Befehlszeile zum folgenden Verzeichnis:

   ```
   cd Installationsverzeichnis/itm/bin
   ```

   Dabei ist *Installationsverzeichnis* das Installationsverzeichnis des Überwachungsagenten. Das Standardinstallationsverzeichnis lautet `/opt/tivoli/tsm/reporting`. Wenn Sie den Überwachungsagenten auf einem vorhandenen IBM Tivoli Monitoring-Server installiert haben, wechseln Sie in das Verzeichnis `bin`. Das Standardinstallationsverzeichnis lautet `/opt/IBM/ITM`.
2. Stoppen Sie die Überwachungsagenteninstanzen, indem Sie einen der folgenden Schritte ausführen:
   - Stoppen Sie die Überwachungsagenten in der grafischen Benutzerschnittstelle von CandleManage, indem Sie die folgenden Befehle ausgeben:
     a. Führen Sie das Programm 'CandleManage' aus, indem Sie die folgenden Befehle ausgeben:

        ```
        ./CandleManage &
        ```

     b. Überprüfen Sie im Fenster **Manage Tivoli Enterprise Monitoring Services**, ob der Überwachungsagent gestoppt wurde. Wurde er nicht gestoppt, wählen Sie die betreffende Agenteninstanz aus, klicken Sie mit der rechten Maustaste auf die Instanz und wählen Sie **Stoppen** aus.
   - Stoppen Sie die Überwachungsagenten über die Befehlszeile, indem Sie die folgenden Befehle ausgeben:
     a. `./itmcmd agent -o Instanzname stop sk`
3. Um sicherzustellen, dass alle Agenten gestoppt wurden, führen Sie die folgenden Schritte aus:
   a. Warten Sie, bis die grafische Schnittstelle von CandleManage zurückmeldet, dass der Agent gestoppt wurde.
   b. Überprüfen Sie, ob der folgende Prozess aktiv ist, indem Sie den folgenden Befehl ausgeben:

```
ps -ef | grep -i SK
```

c. Wenn der Prozess aktiv ist, stoppen Sie ihn, indem Sie den folgenden Befehl ausgeben:

```
kill -9 Prozess-ID
```

4. Lokalisieren Sie das Verzeichnis, in dem die Konfigurationsdateien gespeichert sind, indem Sie den folgenden Befehl ausgeben:

```
Installationsverzeichnis/itm/config
```

5. Um die Tracefunktion für den Überwachungsagenten zu starten, stellen Sie sicher, dass der folgende Wert in der Datei `sk_Agenteninstanz.config` definiert ist:

```
KSK_TRACE='1'
```

Sie müssen auch sicherstellen, dass der folgende Wert in der Konfigurationsdatei `sk.ini` definiert ist:

```
KSK_TRACE=1
```

6. Wenn ein IBM Support-Mitarbeiter Sie zum Aktivieren der Tracefunktion für die API auffordert, stellen Sie sicher, dass der folgende Wert in der Datei `sk_Agenteninstanz.config` definiert ist:

```
KSK_APITRACE='1'
```

Sie müssen auch sicherstellen, dass der folgende Wert in der Konfigurationsdatei `sk.ini` definiert ist:

```
KSK_APITRACE=1
```

7. Starten Sie die Tivoli Monitoring for Tivoli Storage Manager-Agenteninstanzen, indem Sie einen der folgenden Schritte ausführen:
   - Geben Sie in der Befehlszeile die folgenden Befehle aus:

```
cd Installationsverzeichnis/itm/tables
../bin/itmcmd agent -o Instanzname start sk
```

   - Wählen Sie in der grafischen Benutzerschnittstelle von CandleManage jeden Überwachungsagenten aus, klicken Sie mit der rechten Maustaste auf den Agenten und wählen Sie **Starten** aus.

Ergebnisse

Um die Ergebnisse des Trace zu überprüfen, lokalisieren Sie die Protokolldateien im Verzeichnis `/Installationsverzeichnis/itm/logs/`.

Die Protokolldatei, die die Traceinformationen enthält, hat das folgende Format: `aaaapppptttt.log`; der API-Trace hat das folgende Format: `aaaapppptttDsmQuery.out`; dabei ist:

aaaa der Name der Agenteninstanz

pppp die Serveranschlussnummer

tttt die Zeitmarke

Beispiel:

```
Instanzname15001111103143325000.log und Hostname1500DsmQuery.out
```

Trace für den Tivoli Monitoring for Tivoli Storage Manager-Agenten auf einem Windows-Betriebssystem durchführen

Windows

Mithilfe von Tivoli Monitoring for Tivoli Storage Manager können Sie Agenteninstanzen, die IBM Spectrum Protect-Server überwachen, erstellen und konfigurieren. Um die Tracefunktion für die Überwachungsagenten für Server, die unter Windows-Betriebssystemen ausgeführt werden, zu aktivieren, stoppen Sie alle Agenteninstanzen, ändern Sie die Konfigurationsdatei und starten Sie die Agenteninstanzen erneut.

Informationen zu diesem Vorgang

Bevor Sie die Tracefunktion aktivieren, können Sie auch den Tivoli Enterprise Portal-Arbeitsbereich 'Agentenprotokoll' und die Attributgruppe 'Agentenprotokoll' öffnen und die Agentenaktivitäten anzeigen. Der Arbeitsbereich 'Agentenprotokoll' enthält Informationen zu jedem IBM Spectrum Protect-Server, für den eine Agenteninstanz zur Überwachung des Servers konfiguriert ist.

Führen Sie die folgenden Schritte aus, um die Tracefunktion zu aktivieren:

Vorgehensweise

1. Stoppen Sie die Überwachungsagenteninstanzen, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie, während Sie am Tivoli Monitoring-Server arbeiten, auf **Start** > **Alle Programme** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
   b. Wählen Sie jede Überwachungsagenteninstanz aus, klicken Sie mit der rechten Maustaste und wählen Sie **Stoppen** aus.
2. Lokalisieren Sie das Verzeichnis, in dem die Konfigurationsdatei gespeichert ist:

   Installationsverzeichnis\itm\tmaitm6

   Beispiel:

   C:\IBM\itm\tmaitm6
3. Um die Tracefunktion für den Agenten zu starten, stellen Sie sicher, dass der folgende Wert in der Datei kskenv_*Agenteninstanz* definiert ist:

   KSK_TRACE=1
4. Es ist auch möglich, einen Trace für die Anwendungsprogrammierschnittstelle (API) durchzuführen; dies ist jedoch nur erforderlich, wenn ein IBM Support-Mitarbeiter dies anfordert. Um die Tracefunktion für die API zu aktivieren, stellen Sie sicher, dass der folgende Wert in der Datei kskenv_*Agenteninstanz* definiert ist:

   KSK_APITRACE=1
5. Starten Sie die Tivoli Monitoring for Tivoli Storage Manager-Agenteninstanzen, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie, während Sie am Tivoli Monitoring-Server arbeiten, auf **Start** > **Alle Programme** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
   b. Wählen Sie jeden Überwachungsagenten aus, klicken Sie mit der rechten Maustaste und wählen Sie **Starten** aus.

Ergebnisse

Die Ergebnisse des Trace befinden sich in demselben Verzeichnis wie die Konfigurationsdatei:

Installationsverzeichnis\itm\tmaitm6\logs

Die Ergebnisse des API-Trace befinden sich im folgenden Verzeichnis:

Installationsverzeichnis\itm\tmaitm6

Beispiel:

C:\IBM\itm\tmaitm6\logsC:\IBM\itm\tmaitm6

Die Protokolldatei, die die Traceinformationen enthält, hat das Format aaaappppttttt.log; der API-Trace hat das Format aaaapppptttDsmQuery.out; dabei ist:

aaaa der Name der Agenteninstanz

pppp die Serveranschlussnummer

tttt die Zeitmarke

Beispiel:

Instanzname15001111103143325000.log und Hostname1500DsmQuery.out

Kapitel 8. Datenspeicherprobleme beheben

Wenn beim Speichern oder Abrufen von Daten ein Problem auftritt, sind mehrere Methoden zur Behebung des Problems verfügbar.

Probleme mit unlesbaren Daten beheben

Möglicherweise erhalten Sie bei Import- oder Knotenreplikationsprozessen unlesbare Daten, die auf eine fehlende Codepagekonvertierung während dieser Prozesse zurückzuführen sind.

Falls Server mit unterschiedlichen Ländereinstellungen ausgeführt werden, kann es vorkommen, dass einige Informationen in Datenbanken oder in der Systemausgabe unlesbar sind. Beispielsweise könnten in den Kontaktinformationen für die Administrator- und Clientknoten sowie in den Beschreibungen von Maßnahmendomänen ungültige Zeichen angezeigt werden. Hiervon kann jedes Feld betroffen sein, das im Zeichensatz des Servers gespeichert wird und den erweiterten ASCII-Zeichensatz verwendet.

Aktualisieren Sie zur Lösung des Problems nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen **UPDATE**.

Serveraktivitätenprotokoll zur Behebung von Datenspeicherproblemen überprüfen

Überprüfen Sie das Serveraktivitätenprotokoll auf andere Nachrichten, die 30 Minuten vor und 30 Minuten nach dem Fehler aufgetreten sind.

Geben Sie den Befehl **QUERY ACTLOG** aus, um das Aktivitätenprotokoll zu überprüfen. Oft können andere ausgegebene Nachrichten weitere Informationen zur Ursache und Behebung des Fehlers bereitstellen.

Hilfe für Nachrichten überprüfen, die für ein Datenspeicherproblem ausgegeben werden

Überprüfen Sie die Hilfe für alle Nachrichten, die von IBM Spectrum Protect ausgegeben werden.

Die IBM Spectrum Protect-Nachrichten stellen weitere Informationen in den Abschnitten **Erläuterung**, **Systemaktion** und **Benutzeraktion** der Nachricht bereit. Oft können diese ergänzenden Informationen zu der Nachricht die zur Behebung des Problems erforderlichen Schritte bereitstellen.

Datenspeicherproblem reproduzieren

Kann ein Problem einfach oder konsistent reproduziert werden, ist es eventuell möglich, die Ursache des Problems auf eine bestimmte Folge von Ereignissen einzugrenzen.

Probleme beim Lesen oder Schreiben von Daten können sich auf die Reihenfolge der Operationen beziehen, die ausgeführt werden, oder können zu Grunde liegende Einheitenfehler sein.

Typische Probleme in Bezug auf die Reihenfolge von Ereignissen treten bei sequenziellen Datenträgern auf. Beispielsweise kann ein Datenträger für eine Clientsicherung im Gebrauch sein und dieser Datenträger von einer Zurückschreibung der Daten von einem anderen Clientknoten präemptiv verarbeitet werden. Diese Situation kann für die Clientsicherungssitzung, die zurückgestellt wurde, als fehlerhaft erscheinen. Die Clientsicherungssitzung wurde jedoch möglicherweise erfolgreich ausgeführt, wenn sie wiederholt oder nicht zuerst zurückgestellt wurde.

Datenspeicherfehler beheben, die sich auf das Lesen von einer Einheit oder das Schreiben auf eine Einheit beziehen

Falls beim Lesen von Daten von einer Einheit oder beim Schreiben von Daten auf eine Einheit ein Fehler auftritt, zeichnen viele Systeme und Einheiten Informationen in einer Systemfehlerprotokolldatei auf. Beispiele sind die Datei `errpt` bei AIX und die Datei `Event Log` bei Windows.

Wenn eine Einheit oder ein Datenträger, die bzw. der von verwendet wird, einen Fehler an die Systemfehlerprotokolldatei zurückmeldet, handelt es sich wahrscheinlich um einen Einheitenfehler. Die in der Systemfehlerprotokolldatei aufgezeichneten Fehlernachrichten stellen möglicherweise genügend Informationen bereit, um den Fehler zu beheben.

Speicherhierarchie zur Behebung von Datenspeicherproblemen ändern

Die Speicherhierarchie umfasst die definierten Speicherpools und die Beziehungen zwischen den Speicherpools auf dem Server.

Die Speicherpooldefinitionen werden auch vom Speicheragenten verwendet. Wenn Attribute eines Speicherpools geändert wurden, kann die Änderung Auswirkungen auf Datenspeicher- und Abrufoperationen haben. Überprüfen Sie alle Änderungen an der Speicherhierarchie und den Speicherpooldefinitionen. Geben Sie den Befehl **QUERY ACTLOG** aus, um das Protokoll mit Befehlen oder Änderungen anzuzeigen, die möglicherweise Auswirkungen auf Speicherpools haben. Verwenden Sie außerdem die folgenden Befehle **QUERY**, um zu bestimmen, ob Änderungen vorgenommen wurden:

- QUERY STGPOOL F=D

  Überprüfen Sie die Speicherpooleinstellungen. Hat ein Speicherpool den Status UNAVAILABLE, kann auf Daten in diesem Speicherpool nicht zugegriffen werden. Hat ein Speicherpool den Status READONLY, können keine Daten in diesen Pool geschrieben werden. Trifft eine dieser Situationen zu, überprüfen Sie, warum diese Werte definiert wurden, und geben Sie gegebenenfalls den Befehl **UPDATE STGPOOL** aus, um den Pool auf READWRITE zu setzen. Überprüfen Sie auch die Anzahl der Arbeitsdatenträger, die für einen Speicherpool für sequenzielle Datenträger verfügbar sind.
- QUERY DEVCLASS F=D

Die Speicherpools können durch Änderungen an Einheitenklassen beeinflusst werden. Überprüfen Sie die Einheitenklasseneinstellungen für die Speicherpools, einschließlich der Kassettenarchiv-, Laufwerk- und Pfaddefinitionen. Geben Sie die Befehle **QUERY LIBRARY**, **QUERY DRIVE** und **QUERY PATH** für Speicherpools für sequenzielle Datenträger aus.

Servermaßnahmen zur Behebung von Datenspeicherproblemen ändern

Die Servermaßnahmenattribute, die sich direkt auf den Datenspeicher beziehen, sind die Kopiengruppenziele für Sicherungs- und Archivierungskopiengruppen. Außerdem hat die Verwaltungsklasse MIGDESTINATION Auswirkungen darauf, wo Daten gespeichert werden.

Überprüfen Sie alle Änderungen an den Serverspeichermaßnahmen. Geben Sie den Befehl **QUERY ACTLOG** aus, um das Protokoll mit Befehlen oder Änderungen anzuzeigen, die möglicherweise Auswirkungen auf Speichermaßnahmen haben. Verwenden Sie außerdem die folgenden Befehle **QUERY**, um zu bestimmen, ob Änderungen vorgenommen wurden:

- QUERY COPYGROUP F=D

  Überprüfen Sie die Einstellungen von DESTINATION für die Kopiengruppen TYPE=BACKUP und TYPE=ARCHIVE. Überprüfen Sie außerdem das "Umlagerungsziel" für Verwaltungsklassen, die von HSM-Clients verwendet werden. Wenn Speicherpoolzielorte geändert wurden und nachfolgende Datenlese- oder -schreiboperationen jetzt fehlschlagen, überprüfen Sie entweder die vorgenommenen Änderungen und korrigieren Sie den Fehler oder setzen Sie die Werte auf die vorherigen Einstellungen zurück.
- QUERY NODE F=D

  Die Zuordnung eines Knotens zu einer anderen Domäne kann Auswirkungen auf Datenlese- und -schreiboperationen für diesen Client haben. Der Knoten kann jetzt möglicherweise Speicherpoolzielorten zugeordnet sein, die auf der Basis der Anforderungen für diesen Knoten nicht geeignet sind. Beispielsweise könnte der Knoten einer Domäne zugeordnet sein, die über keine Kopiengruppenziele TYPE=ARCHIVE verfügt. Wenn dieser Knoten versucht, Daten zu archivieren, schlägt die Operation fehl.

Datenspeichersicherungs- oder -kopierproblem beheben, das nur bei einem bestimmten Knoten auftritt

Wenn Sie keine Daten auf einen bestimmten Knoten sichern oder kopieren können, ist möglicherweise ein Pool für aktive Daten nicht unter den aktiven Zielorten aufgelistet. Diese sind in der Maßnahmendomäne des Knotens angegeben.

Geben Sie den Befehl `QUERY NODE` *`Knotenname`* `F=D` aus, um zu überprüfen, ob der Knoten, der die Daten speichert, berechtigt ist. Mit dem Befehl **QUERY NODE** wird der Name der Maßnahmendomäne gefunden, der der Knoten zugeordnet ist. Geben Sie den Befehl `QUERY DOMAIN` *`Domänenname`* aus, wobei *Domänenname* die Ausgabe des vorherigen Befehls **QUERY NODE** ist. Suchen Sie unter dem Parameter **ACTIVEDESTINATION** nach der Liste der Pools für aktive Daten. Ist der Pool für aktive Daten, in dem die Daten gespeichert werden sollen, nicht in der Liste, geben Sie den Befehl **UPDATE DOMAIN** aus, um der Liste den Pool für aktive Daten hinzuzufügen.

Datenspeicherproblem beheben, das nur bei einem bestimmten Datenträger auftritt

Wenn Probleme nur bei einem bestimmten Speicherdatenträger auftreten, liegt möglicherweise ein Fehler beim Datenträger selbst vor. Der Fehler kann darauf beruhen, ob es sich bei dem Datenträger um einen sequenziellen Datenträger oder einen Datenträger des Typs DISK handelt.

Ist Ihre Operation eine Datenschreiboperation, geben Sie den Befehl `UPDATE VOLUME` *`Datenträgername`* `ACCESS=READONLY` aus, um diesen Datenträger auf READONLY zu setzen. Wiederholen Sie dann die Operation. Ist die Operation erfolgreich, setzen Sie den Originaldatenträger wieder auf READWRITE, indem Sie den Befehl `UPDATE VOLUME` *`Datenträgername`* `ACCESS=READWRITE` ausgeben. Wiederholen Sie anschließend die Operation. Schlägt die Operation nur bei Verwendung dieses Datenträgers fehl, geben Sie gegebenenfalls den Befehl **`AUDIT VOLUME`** aus, um diesen Datenträger zu prüfen, und geben Sie den Befehl **`MOVE DATA`** aus, um die Daten von diesem Datenträger auf andere Datenträger in dem Speicherpool zu versetzen. Nachdem die Daten von diesem Datenträger versetzt wurden, löschen Sie den Datenträger, indem Sie den Befehl **`DELETE VOLUME`** ausgeben.

Hinweise und Tipps für die Speicherung

Die hier zusammengestellten Hinweise und Tipps stammen aus tatsächlichen Problemfällen. Möglicherweise eignet sich eine der Lösungen für die Behebung Ihres IBM Spectrum Protect-Problems.

Hinweise und Tipps zum Einheitentreiber

Probleme mit dem Einheitentreiber können durch das Betriebssystem, die Anwendung, die die Einheit verwendet, die Firmware der Einheit oder die Hardware der Einheit selbst verursacht werden.

Wenn ein Problem mit einer Einheit festgestellt wird, stellen Sie immer die Frage „Wurden Änderungen vorgenommen?"

Wenn die Adapterfirmware geändert wurde, können auf einer Einheit intermittierende oder permanente Fehler auftreten. Versuchen Sie, eine frühere Version der Firmware zu verwenden, um zu bestimmen, ob der Fehler bestehen bleibt.

Wurde die Verkabelung zwischen dem Computer und der Einheit geändert, können oft intermittierende oder permanente Fehler die Folge sein. Überprüfen Sie die Änderungen an der Verkabelung, um sicherzustellen, dass die Verkabelung korrekt ist.

Auf einer Einheit können intermittierende oder permanente Fehler auftreten, wenn die Firmware der Einheit geändert wurde. Versuchen Sie, eine frühere Version der Firmware zu verwenden, um zu bestimmen, ob der Fehler bestehen bleibt.

Bei SCSI-Verbindungen kann ein verbogener Kontaktstift in dem SCSI-Kabel, das an den Computer (oder die Einheit) angeschlossen wird, zu Fehlern bei dieser Einheit oder einer anderen Einheit an demselben SCSI-Bus führen. Ein Kabel mit einem verbogenen Kontaktstift muss repariert oder ausgetauscht werden. Genauso müssen SCSI-Busse abgeschlossen sein. Ist ein SCSI-Bus nicht ordnungsgemäß abgeschlossen, können auf Einheiten an dem Bus intermittierende Fehler auftreten,

oder Daten, die an den Bus übertragen werden, können beschädigt sein oder als beschädigt erscheinen. Überprüfen Sie die Abschlussstecker am SCSI-Bus, um sicherzustellen, dass sie fehlerfrei sind.

Hinweis: Wenn die Informationen in „Hinweise und Tipps" das Problem mit Ihrem Einheitentreiber nicht beheben oder wenn es sich um die Erstkonfiguration des Einheitentreibers Ihres Systems handelt, überprüfen Sie, ob Ihre Hardwareeinheiten unterstützt werden. Lesen Sie die Informationen im Support Portal.

Anpassung an Betriebssystemänderungen

Die Betriebssystemwartung kann Kernel-Level, Einheitentreiber oder andere Systemattribute ändern, die eine Einheit beeinflussen können.

Genauso kann ein Upgrade der Version oder des Releases des Betriebssystems Einheitenkompatibilitätsprobleme verursachen. Falls möglich, setzen Sie das Betriebssystem auf den Status vor dem Einheitenfehler zurück. Falls das nicht möglich ist, überprüfen Sie, ob für diese Fixversion, dieses Release oder diese Version des Betriebssystems Einheitentreiberaktualisierungen erforderlich sind.

Anpassung an Änderungen des mit der Einheit verbundenen HBA- oder SCSI-Adapters

Ein Einheitentreiber kommuniziert mit einer bestimmten Einheit über einen Adapter.

Wenn es sich um eine über Fibre Channel angeschlossene Einheit handelt, verwendet der Einheitentreiber einen Hostbusadapter (HBA) für die Kommunikation. Wenn die Einheit über einen SCSI-Anschluss verfügt, verwendet der Einheitentreiber einen SCSI-Adapter für die Kommunikation. In beiden Fällen, kann der Einheitentreiber Probleme bei der Verwendung der Einheit haben, wenn die Adapterfirmware aktualisiert oder der Adapter selbst ausgetauscht wurde.

Wenden Sie sich an den Anbieter des Adapters, um zu überprüfen, ob er ordnungsgemäß installiert und konfiguriert ist. Die folgende Liste enthält die anderen möglichen Schritte:

- Wenn der Adapter geändert wurde, versuchen Sie, den vorherigen Adapter wiederherzustellen, um zu bestimmen, ob das Problem behoben ist.
- Wenn andere Hardware in dem Computer geändert oder wenn der Computer geöffnet wurde, öffnen Sie den Computer erneut und überprüfen Sie, ob der Adapter richtig in dem Bus sitzt. Durch das Öffnen und Ändern anderer Hardware in dem Computer können sich die Karten und andere Anschlüsse in dem Computer gelöst haben, was sporadisch auftretende Probleme oder einen vollständigen Ausfall von Einheiten oder anderen Systemressourcen verursachen kann.

Lose Kabelverbindung beseitigen

Wenn eine Verbindung von der Einheit zum Kabel oder vom Kabel zur Einheit lose ist, könnten Probleme mit einer Einheit auftreten.

Überprüfen Sie die Anschlüsse und stellen Sie sicher, dass die Kabelverbindungen korrekt und sicher sind.

Bei SCSI-Einheiten überprüfen Sie, ob die SCSI-Abschlussstecker korrekt sind und ob es verbogene Kontaktstifte im Abschlussstecker selbst gibt. Ein nicht ordnungsgemäß abgeschlossener SCSI-Bus kann zu schwerwiegenden Problemen mit Einheiten in diesem Bus führen.

Fehlernachrichten im Systemfehlerprotokoll

Eine Einheit kann versuchen, einen Fehler in einem Systemfehlerprotokoll aufzulisten.

Die folgenden Beispiele zeigen verschiedene Systemfehlerprotokolle:

- AIX `errpt`
- Windows `Ereignisprotokoll`

Die Systemfehlerprotokolle können nützlich sein, weil die aufgezeichneten Nachrichten und Informationen für einen Fehlerbericht hilfreich sein können oder weil die Nachrichten Empfehlungen zur Fehlerbehebung enthalten können.

Überprüfen Sie das entsprechende Fehlerprotokoll und führen Sie Aktionen auf Basis der im Fehlerprotokoll ausgegebenen Nachrichten durch.

32-Bit- oder 64-Bit-Linux-Kernelmodule für 32-Bit- oder 64-Bit-Anwendungen unterstützen

Linux

Die Linux-Kernelmodule steuern den Bitmodus der generischen Linux-SCSI-Einheitentreiber, alle anderen HBA-Treiber (HBA - Hostbusadapter) und andere Einstellungen.

Alle diese Kernelmodule unterstützen nur Anwendungen, die denselben Bitmodus wie aktive Kernelmodule aufweisen. Das heißt, 64-Bit-Kernelmodule unterstützen nur 64-Bit-Anwendungen auf 64-Bit-Linux-Systemen.

Wenn eine 32-Bit-Anwendung auf einem 64-Bit-Linux-System ausgeführt wird und ein 64-Bit-Kernelmodul aufruft, verursacht die 32-Bit-Anwendung einen Kernelsegmentierungsfehler. Ein Segmentierungsfehler tritt auch dann auf, wenn eine 64-Bit-Anwendung ein 32-Bit-Kernelmodul auf einem 32-Bit-Linux-System aufruft.

Zur Vermeidung dieser Segmentierungsfehler müssen Sie sicherstellen, dass der Bitmodus des Linux-Kernelmoduls und seiner Anwendungen identisch ist, indem Sie verifizieren, dass die 32-Bit-Anwendungen nur 32-Bit-Kernelmodule auf 32-Bit-Linux-Systemen aufrufen können und 64-Bit-Anwendungen nur 64-Bit-Kernelmodule auf 64-Bit-Linux-Systemen aufrufen können.

IBM Spectrum Protect-Server unter Linux in einer x86_64-Architektur ausführen

Linux

Die 32-Bit- und 64-Bit-Linux-Betriebssysteme können auf den AMD64- und EM64T-Systemen (64-Bit-Systeme) ausgeführt werden.

Ein IBM Spectrum Protect-64-Bit-Server und -Speicheragent unter Linux können nur auf einem AMD64/EM64T-System mit einem 64-Bit-Linux-Betriebssystem ausgeführt werden. Ein IBM Spectrum Protect-32-Bit-Server und -Speicheragent unter Linux können nur auf einem AMD64/EM64T-System mit einem 32-Bit-Linux-Betriebssystem ausgeführt werden.

Ein IBM Spectrum Protect-64-Bit-Server, der den Befehl **QUERY SAN** ausgibt, erfordert eine 64-Bit-HBA-API auf einem AMD64/EM64T-System. Wenn ein AMD64-System mit einem Qlogic-HBA ausgestattet ist, kann ein Fehler auftreten, weil Qlogic standardmäßig nur eine 32-Bit-HBA-API auf dem AMD64-System bereitstellt.

Sie müssen die 64-Bit-HBA-API auf dem System installieren, bevor der 64-Bit-Befehl **QUERY SAN** ausgegeben wird.

Anpassung an HBA-Treiberänderungen in den Linux 2.6.x-Kerneln

Die deutlichste Änderung für HBA-Treiber in den Linux 2.6.x-Kerneln ist die, dass alle Treiber das neue Suffix „ko" aufweisen.

Die folgende Liste enthält die Treibernamen und -positionen in 2.6.x-Kerneln:

Adaptec
: Der Treiber (`aic7xxx.ko`) befindet sich im Verzeichnis `/lib/modules/kernel-level/drivers/scsi/aic7xxx/`.

Emulex
: Der Treiber (`lpfcdd.ko`) befindet sich im Verzeichnis `/lib/modules/kernel-level/drivers/scsi/lpfc/`.

Qlogic
: Die Treibernamen lauten `qla2xxx.ko`, `qla2100.ko`, `qla2200.ko`, `qla2300.ko`, `qla2322.ko` usw. Die HBA-Treiber müssen in einer bestimmten Reihenfolge geladen werden. `qla2xxx.ko` ist ein Basistreiber und muss zuerst geladen werden. Nach dem Laden des Treibers `qla2xxx.ko` sollte das System den Treiber `qla2300.ko` laden, wenn es mit einer Qla2300-Karte ausgestattet ist. Alle Treiber befinden sich im Verzeichnis `/lib/modules/kernel-level/drivers/scsi/qla2xxx/`.

Unterstützung mehrerer Nummern logischer Einheiten in Linux-Kerneln aktivieren

Linux

Damit SCSI-Einheiten mit mehreren LUNs (Logical Unit Number, Nummer der logischen Einheit) auf einem Linux-System konfiguriert werden können, muss der Linux-Kernel für die Unterstützung mehrerer LUNs konfiguriert sein.

Die Unterstützung mehrerer LUNs ist bei einigen Linux-Varianten jedoch keine Standardoption. In diesem Fall müssen Benutzer diese Option manuell zum aktiven Kernel hinzufügen. Gehen Sie wie folgt vor, um die Unterstützung mehrerer LUNs in der IA32-Architektur zu konfigurieren und zu aktivieren:

1. Fügen Sie einen Parameter zu einer Konfigurationsdatei für Bootladeprogramme hinzu.
   - Für Bootladeprogramm LILO:
     a. Fügen Sie append=„max_scsi_luns=128" zur Datei `/ect/lilo.conf` hinzu.
     b. Führen Sie lilo aus.
   - Für Bootladeprogramm GRUB:
     a. Fügen Sie max_scsi_luns=128 hinter der Kernel-Image-Liste in Datei `/etc/grub.conf` für RedHat-Verteilungen hinzu.
     b. Fügen Sie max_scsi_luns=128 hinter der Kernel-Image-Liste in Datei `/boot/grub/menu.1` für SuSE-Verteilungen hinzu.
2. Starten Sie das System erneut.

IBM Spectrum Protect zur Ausführung von ddtrace unter Linux verwenden

Linux

Für den Durchgriffseinheitentreiber kann ein Trace mithilfe des Befehls **DDTRACE** durchgeführt werden.

Geben Sie die folgenden Befehle über die Serverkonsole oder den Verwaltungsclient aus, um den Trace zu aktivieren:

```
trace enable lpdd <andere Server-Traceklassennamen>
trace begin <Dateiname>
```

Wählen Sie eine der drei folgenden Optionen aus:

- ddtrace start librarydd tapedd (Kassettenarchiv- und Laufwerktrace)
- ddtrace start librarydd (nur Kassettenarchivtrace)
- ddtrace start tapedd (Nur Laufwerktrace)

Hinweis: **DDTRACE GET** und **DDTRACE END** sind nicht erforderlich.

Der Trace für den IBM Spectrum Protect-Durchgriffseinheitentreiber kann nicht durch das Dienstprogramm ddtrace aktiviert werden.

Einheitendaten von Hostsystemen in einem dynamischen Speicherbereichsnetz (SAN) ohne Neustart aktualisieren

Wenn sich Einheiten in einer SAN-Umgebung ändern, werden die Informationen zu dieser geänderten Umgebung nicht automatisch an Hostsysteme mit SAN-Anschluss gesendet.

Wenn die Einheitendaten für Hostsysteme, die an das SAN angeschlossen sind, nicht aktualisiert wurden, sind die zuvor definierten Einheitenpfade nicht mehr vorhanden. Wenn Sie die vorhandenen Einheitendaten für die Definition von Einheitenpfaden oder zum Sichern oder Zurückschreiben von Daten verwenden, können diese Operationen fehlschlagen. Zur Vermeidung dieser Art von Fehlern sollten Sie für jedes Betriebssystem eine andere Methode verwenden, um die Einheitendaten im SAN ohne einen Neustart des Hostsystems zu aktualisieren.

AIX Geben Sie den Befehl **CFGMGR** aus, um das Betriebssystem zu zwingen, sich selbst neu zu konfigurieren. Führen Sie dann SMIT aus, um Ihre IBM Spectrum Protect-Einheiten neu zu konfigurieren.

Linux Es gibt keinen Systembefehl zur Neukonfiguration des Betriebssystems. Zur erneuten Überprüfung der SCSI-Busse und Fibre-Channels müssen die Adaptertreiber, die diesen SCSI-Adaptern und Fibre-Channel-Adaptern entsprechen, entladen und dann erneut in den Linux-Kernel geladen werden. Führen Sie das Dienstprogramm **autoconf** oder den Befehl **TSMSCSI** nach dem erneuten Laden von HBA-Treibern aus, um IBM Spectrum Protect-Einheiten unter Linux neu zu konfigurieren. Sie könnten den Befehl **LSPCI** ausgeben, um festzustellen, welcher SCSI-Adapter und Fibre-Channel-Adapter auf dem System verfügbar ist. Der Befehl **RMMOD** entlädt einen Treiber aus dem Kernel und der Befehl **MODPROBE** lädt einen Treiber in den Kernel.

Tabelle 14. Hostbusadapter und entsprechende Treiber für Linux-Architekturen

Hostbusadapter (HBA)	HBA-Treibername	Verfügbare Architekturen
Adaptec 7892	aix7xxx	IA32, AMD64

Tabelle 14. Hostbusadapter und entsprechende Treiber für Linux-Architekturen (Forts.)

Hostbusadapter (HBA)	HBA-Treibername	Verfügbare Architekturen
Qlogic 22xx	qla2200	IA32, AMD64
Qlogic 23xx	qla2300	IA32, AMD64
Qlogic 2362	qla2362	EM64T
Emulex	lpfcdd	IA32, iSeries, pSeries

Option 'Multiple LUN' für Adaptec SCSI und Qlogic Fibre-Channel HBA BIOS-Einstellungen unter Linux auf „on" setzen

Standardmäßig setzen Adaptec SCSI-Adapter die Option 'Multiple LUN' (LUN = Nummer der logischen Einheit) in ihren BIOS-Einstellungen auf „off"; dies verhindert, dass der SCSI-Adaptertreiber eine SCSI-Einheit mit mehreren LUNs korrekt prüfen kann.

Vorgehensweise

Die Option 'Multiple LUN' muss aktiviert (auf 'on' gesetzt) werden. Führen Sie die folgenden Schritte aus, um die Option 'Multiple LUN' zu aktivieren:

1. Drücken Sie gleichzeitig die Steuertaste (Strg) und die Taste A.
2. Wählen Sie **SCSI Device Configuration** unter der Einstellung **Configure/View Host Adapter** aus.
3. Ändern Sie den Wert für 'BIOS Multiple LUN Support' von 'No' in 'Yes'.

Option 'Tape enable' aktivieren:

Standardmäßig inaktivieren Qlogic Fibre-Channel-Hostbusadapter die Option 'Tape enable' in ihren BIOS-Einstellungen; dies wirkt sich auf die Ausführung einiger SCSI-Befehle auf mehreren SCSI-Bandeinheiten aus.

Vorgehensweise

Die Option 'Tape enable' muss aktiviert werden. Führen Sie die folgenden Schritte aus, um die Option 'Tape enable' zu aktivieren.

1. Drücken Sie gleichzeitig die Tasten Alt und Q.
2. Wählen Sie **Advanced Settings** aus.
3. Ändern Sie den Wert für 'Fibre Channel Tape Support' von 'Disable' in 'Enable'.

Hinweise und Tipps zu Festplattenlaufwerken und Plattensubsystemen

Der IBM Spectrum Protect-Server benötigt für eine bestimmte Ausführungsweise Festplattenlaufwerke, Plattensubsysteme, vom Hersteller erworbene Dateisysteme und ferne Dateisysteme. Dadurch wird es IBM Spectrum Protect ermöglicht, Daten auf geeignete Weise zu verwalten und zu speichern, wobei die Integrität des Servers selbst sichergestellt wird.

Die folgenden Definitionen werden zum besseren Verständnis von Festplattenlaufwerken und Plattensubsystemen bereitgestellt:

Festplattenlaufwerk
Ein Festplattenlaufwerk ist eine Speichereinheit, die für gewöhnlich inner-

halb eines bestimmten Computers installiert und von einem IBM Spectrum Protect-Server zum Speichern von Daten auf diesem Computer verwendet wird.

Plattensubsystem
Ein externes Plattensubsystem ist mit einem Computer über ein SAN (Speicherbereichsnetz) oder einen anderen Mechanismus verbunden. Im Allgemeinen befinden sich Plattensubsysteme außerhalb des Computers, mit dem sie verbunden sind. Sie können sich in unmittelbarer Nähe oder in größerer Entfernung befinden. Diese Subsysteme können auch über eine Methode zum Zwischenspeichern der Ein-/Ausgabeanforderungen auf den Platten verfügen. Wenn Daten zwischengespeichert werden, können trotz einer Anforderung zur Cacheumgehung, die auf fernen Dateisystemen und bestimmten Plattensubsystemen auftreten kann, Ein-/Ausgabefehler die Folge sein. Die Fehler werden aufgrund einer Abweichung zwischen der Aufzeichnung in IBM Spectrum Protect und den Daten, die tatsächlich in einem Dateisystem resident sind, verursacht. Ferne Dateisysteme und Plattensubsysteme, die diese Merkmale aufweisen, werden nicht unterstützt. Plattensubsysteme verfügen oft über ihre eigene Konfigurations- und Verwaltungssoftware. Ein Plattensubsystem muss die Ergebnisse synchron zurückmelden.

Der Server kann die von dem Computer oder Betriebssystem verwendeten Festplattenlaufwerke und Plattensubsysteme auf dem Computer definieren, auf dem IBM Spectrum Protect installiert ist. Normalerweise wird ein Festplattenlaufwerk oder Plattensubsystem für den Computer, auf dem IBM Spectrum Protect installiert ist, als Laufwerk oder Dateisystem definiert. Nachdem das Festplattenlaufwerk oder Plattensubsystem für das Betriebssystem definiert wurde, kann IBM Spectrum Protect diesen Speicherplatz verwenden, indem eine Datenbank, ein Wiederherstellungsprotokoll oder ein Speicherpooldatenträger auf der Einheit zugeordnet wird. Der IBM Spectrum Protect-Datenträger sieht dann wie eine andere Datei auf diesem Laufwerk oder Dateisystem aus.

Cacheumgehung während der Ausführung von Schreiboperationen

Datenbank-, Wiederherstellungsprotokoll- und Speicherpooldatenträger werden mit den entsprechenden Betriebssystemeinstellungen geöffnet, um sicherzustellen, dass Datenschreibanforderungen den Cache umgehen und Daten direkt auf die Einheit geschrieben werden.

Durch die Cacheumgehung während der Ausführung von Schreiboperationen wird die Integrität von Clientattributen und Daten von IBM Spectrum Protect aufrecht erhalten. Die Umgehung des Cache ist erforderlich. Wenn bei einem externen Ereignis (z. B. bei einem Stromausfall) der Server oder der Computer, auf dem der Server installiert ist, angehalten oder unterbrochen wird, während der Server aktiv ist, werden die Daten im Cache möglicherweise auf die Platte geschrieben oder nicht. Wenn die IBM Spectrum Protect-Daten im Plattencache nicht erfolgreich auf die Platte geschrieben werden, sind die Informationen in der Serverdatenbank oder in dem Wiederherstellungsprotokoll möglicherweise nicht vollständig. Außerdem sind Daten, von denen angenommen wurde, dass sie auf die Speicherpooldatenträger geschrieben wurden, möglicherweise nicht vorhanden.

Bei Festplattenlaufwerken, die auf dem Computer installiert sind, auf dem der Server installiert und aktiv ist, ist die Cacheumgehung nicht von so großer Bedeutung. In diesem Fall steuern die Betriebssystemeinstellungen, die verwendet werden, wenn IBM Spectrum Protect Datenträger auf diesem Festplattenlaufwerk

öffnet, im Allgemeinen das entsprechende Cacheverhalten und berücksichtigen die Anforderung zum Verhindern des Caching von Schreiboperationen.

Normalerweise ist die Verwendung und Konfiguration des Caching für Plattensubsysteme ein größeres Problem, da Plattensubsysteme oft keine Informationen zur Cacheumgehung für Schreiboperationen vom Betriebssystem erhalten. Möglicherweise werden diese Informationen auch von Plattensubsystemen ignoriert, wenn ein Datenträger geöffnet wird. Daher kann das Caching von Datenschreiboperationen zu einer Beschädigung der Serverdatenbank und/oder zu einem Verlust von Clientdaten führen. Die Probleme sind von den IBM Spectrum Protect-Datenträgern, die auf dem Plattensubsystem definiert sind, und dem Datenvolumen, das im Cache verloren gegangen ist, abhängig. Plattensubsysteme sollten nicht für das Caching von Schreiboperationen konfiguriert werden, wenn ein IBM Spectrum Protect-Datenbank-, -Wiederherstellungsprotokoll- oder -Speicherpooldatenträger auf dieser Platte definiert ist. Eine Alternative ist die Verwendung von nicht flüchtigem Cache für das Plattensubsystem. Bei nicht flüchtigem Cache wird eine Notstromversorgung oder eine andere Methode verwendet, die es ermöglicht, dass der Inhalt des Cache auf die Platte geschrieben wird, wenn ein Fehler auftritt.

Vorhandene Daten auf andere Datenträger versetzen, bevor die Datenbank geändert oder versetzt wird

Die Größe und Position von IBM Spectrum Protect-Speicherpooldatenträgern (Dateien) können nicht geändert werden, nachdem sie vom Server definiert und verwendet wurden.

Wenn die Größe geändert oder die Datei versetzt wird, stimmen interne Informationen, die IBM Spectrum Protect zum Beschreiben des Datenträgers verwendet, möglicherweise nicht mehr mit den tatsächlichen Attributen der Datei überein. Wenn Sie einen IBM Spectrum Protect-Speicherpooldatenträger versetzen oder die Größe ändern müssen, versetzen Sie alle vorhandenen Daten auf andere Datenträger, bevor Sie die Datenbank ändern oder versetzen.

FILE-Verzeichniszuordnung zwischen Speicheragenten und Servern für gemeinsam genutzte Dateien

IBM Spectrum Protect-Server und -Speicheragenten können auf dieselben Daten in der Einheitenklasse FILE zugreifen, indem eine Gruppe von Verzeichnissen definiert werden, die in einer Einheitenklassendefinition verwendet werden sollen.

Der Verzeichnisname in einer Definition der Einheitenklasse FILE gibt die Position an, an der der Server die Dateien einfügt, die Speicherdatenträger für die Einheitenklasse darstellen. Wenn Sie den Befehl **DEFINE DEVCLASS** ausgeben, erweitert der Server den angegebenen Verzeichnisnamen in sein vollständig qualifiziertes Format (ab Stammverzeichnis).

Sie können mindestens ein Verzeichnis als Speicherposition der in der Einheitenklasse FILE verwendeten Dateien angeben. Die Standardposition ist das aktuelle Arbeitsverzeichnis des Servers zum Zeitpunkt der Befehlseingabe. Sie können die Verzeichnisse für AIX oder Linux angeben.

Geben Sie nicht mehrere Verzeichnisse aus demselben Dateisystem an, da dies zu falschen Speicherplatzberechnungen führen kann. Befinden sich die Verzeichnisse `/usr/dir1` und `/usr/dir2` beispielsweise in demselben Dateisystem, wird bei einer Überprüfung des Speicherbereichs jedes Verzeichnis als separates Dateisystem gezählt. Während der Ausführung von Speicheroperationen wird bei der Überprüfung des Speicherbereichs eine vorläufige Auswertung des verfügbaren Speicherplatzes durchgeführt. Wenn die Speicherbereichsberechnungen falsch sind, führt

der Server möglicherweise eine COMMIT-Operation für einen Speicherpool des Typs FILE aus, obwohl er keinen Speicherbereich abrufen kann, wodurch die Operation fehlschlägt. Ist die Überprüfung des Speicherbereichs korrekt, kann der Server den Pool des Typs FILE in der Speicherhierarchie überspringen und den nächsten Speicherpool verwenden, wenn er verfügbar ist.

Wenn der Server einen Arbeitsdatenträger zuordnen muss, erstellt er eine neue Datei in dem angegebenen Verzeichnis bzw. den angegebenen Verzeichnissen. (Der Server kann jedes der Verzeichnisse auswählen, in denen neue Arbeitsdatenträger erstellt werden sollen.) Um die Leistung zu optimieren, stellen Sie sicher, dass mehrere Verzeichnisse separaten physischen Datenträgern entsprechen.

Die folgende Tabelle enthält die Dateinamenerweiterungen, die der Server für Arbeitsdatenträger erstellt. Sie richten sich nach dem Typ der gespeicherten Daten.

Tabelle 15. Dateinamenerweiterungen für Arbeitsdatenträger

Auf dem Arbeitsdatenträger gespeicherte Daten	**Dateinamenerweiterung**
Clientdaten	`.BFS`
Export	`.EXP`
Datenbanksicherung	`.DBV`

Für jeden Speicheragenten, der **FILE**-Zugriff gemeinsam nutzt, müssen die Pfade (**PATH**), die für jedes vom Speicheragenten erkannte Laufwerk (**DRIVE**) definiert sind, Zugriff auf dieselbe Verzeichnisgruppe bereitstellen. Wenn die Pfade (mit **PATH**) definiert werden, müssen die Verzeichnisse für jeden Speicheragenten in Anzahl und Reihenfolge mit den in der Einheitenklassendefinition auf dem Server aufgelisteten Verzeichnissen übereinstimmen. Wenn diese Definitionen nicht übereinstimmen, kann der Speicheragent möglicherweise nicht auf die FILE-Datenträger zugreifen, was erfolgreiche LAN-Zurückschreibungen und Ladefehler für LAN-unabhängige Zurückschreibungsoperationen zur Folge haben kann.

Hinweise und Tipps zu Bandlaufwerken und -archiven

Probleme mit Bandlaufwerken und -archiven können durch die Software auf dem Computer, der die Einheit verwenden will, durch Verbindungen zu der Einheit oder durch die Einheit verursacht werden.

Wenn ein Problem mit einer Einheit festgestellt wird, stellen Sie immer die Frage „Wurden Änderungen vorgenommen?" Ziehen Sie alle Fehlerquellen auf dem Computer in Betracht, der die Einheit verwenden will, oder überprüfen Sie die Einheit selbst. Dies gilt besonders dann, wenn die Einheit vor einer bestimmten Änderung funktioniert hat, dann aber nach der Änderung nicht mehr funktioniert hat.

- Wenn die Adapterfirmware geändert wurde, können auf einer Einheit intermittierende oder permanente Fehler auftreten. Versuchen Sie, eine frühere Version der Firmware zu verwenden, um zu bestimmen, ob der Fehler bestehen bleibt.
- Wurde die Verkabelung zwischen dem Computer und der Einheit geändert, können intermittierende oder permanente Fehler auftreten. Überprüfen Sie die Änderungen an der Verkabelung, um sicherzustellen, dass die Verkabelung korrekt ist.
- Wenn die Einheitenfirmware geändert wurde, können auf einer Einheit intermittierende oder permanente Fehler auftreten. Versuchen Sie, eine frühere Version der Firmware zu verwenden, um zu bestimmen, ob der Fehler bestehen bleibt.

Anpassung an Betriebssystemänderungen

Die Betriebssystemwartung kann Kernel-Level, Einheitentreiber oder andere Systemattribute ändern, die eine Einheit beeinflussen können. Genauso kann ein Upgrade der Version oder des Releases des Betriebssystems Einheitenkompatibilitätsprobleme verursachen.

Falls möglich, setzen Sie das Betriebssystem auf den Status vor dem Einheitenfehler zurück. Kann das Betriebssystem nicht zurückgesetzt werden, überprüfen Sie, ob für die Fixversion, das Release oder die Version des Betriebssystems Einheitentreiberaktualisierungen erforderlich sind.

Anpassung an Einheitentreiberänderungen

Ein Upgrade für einen Einheitentreiber kann zur Folge haben, dass ein Bandlaufwerk oder ein Speicherarchiv nicht arbeitet. Diese Probleme können auch aufgrund des Typs des Treibers auftreten, der verwendet wird.

Bei der Arbeit mit IBM Speicherarchiven oder Laufwerken ist im Gegensatz zur Verwendung von Speicherarchiven und Laufwerken anderer Hersteller der ausgewählte Typ des Einheitentreibers wichtig. IBM Speicherarchive und Laufwerke sollten den IBM Einheitentreiber verwenden, während Speicherarchive und Laufwerke anderer Hersteller den IBM Spectrum Protect-Einheitentreiber verwenden sollten.

Kehren Sie zur vorherigen (oder früheren) Version des Einheitentreibers zurück, um zu bestimmen, ob das Problem durch die neuere Version des Treibers verursacht wurde.

Anpassung an einen ersetzten Adapter oder an andere Hardwareänderungen

Eine SCSI-Verbindung (SCSI = Small Computer System Interface) zur Einheit verwendet einen SCSI-Adapter. Eine Fibre-Channel-Verbindung (optisch) zur Einheit verwendet einen Hostbusadapter (HBA).

In beiden Fällen kann das Problem durch einen geänderten Adapter oder einen offenen Computer, in dem andere Hardware geändert oder fixiert wurde, verursacht werden.

Hinweis: Der Verbindungspunkt der Einheit zum Computer wird als Adapter bezeichnet. Ein anderer Begriff für Adapter ist *Karte*.

Lesen Sie die folgenden Informationen, die Ihnen bei der Anpassung an einen ersetzten Adapter oder an andere geänderte Hardware helfen:

- Wenn der Adapter geändert wurde, kehren Sie zum vorherigen Adapter zurück, um zu bestimmen, ob das Problem behoben ist.
- Wenn Hardware in dem Computer geändert oder der Computer geöffnet wurde, überprüfen Sie den Computer, um sicherzustellen, dass der Adapter ordnungsgemäß in dem Bus sitzt. Durch das Öffnen und Ändern anderer Hardware in dem Computer können sich die Karten und andere Anschlüsse in dem Computer gelöst haben, was sporadisch auftretende Probleme oder einen vollständigen Ausfall von Einheiten oder anderen Systemressourcen verursachen kann.

Lose Kabelverbindung beseitigen

Probleme mit der Einheit können auftreten, wenn ein Anschluss vom Computer zum Kabel oder vom Kabel zur Einheit lose ist.

Überprüfen Sie die Anschlüsse und stellen Sie sicher, dass die Kabelverbindungen korrekt und sicher sind.

Bei SCSI-Einheiten überprüfen Sie, ob die SCSI-Abschlussstecker korrekt sind und ob es verbogene Kontaktstifte im Abschlussstecker selbst gibt. Ein nicht ordnungsgemäß abgeschlossener SCSI-Bus kann zu Problemen mit Einheiten in diesem Bus führen.

Fehlernachrichten zur Behebung einer Einheitenstörung verwenden

Eine Einheit kann einen Fehler an ein Systemfehlerprotokoll zurückmelden, das Sie verwenden können, um die Fehlerursache zu bestimmen.

Beispiele für verschiedene Systemfehlerprotokolle sind:

- `errpt` für AIX
- `Ereignisprotokoll` für Windows

Die Systemfehlerprotokolle können nützlich sein, weil die aufgezeichneten Nachrichten und Informationen bei der Zurückmeldung des Fehlers hilfreich sein können oder weil die Nachrichten Empfehlungen zur Fehlerbehebung enthalten können. Überprüfen Sie das entsprechende Fehlerprotokoll und führen Sie alle empfohlenen Aktionen auf der Basis der im Fehlerprotokoll ausgegebenen Nachrichten aus.

Hinweise und Tipps zum Speicherbereichsnetz

Probleme mit einem Speicherbereichsnetz (SAN) können durch die Software auf dem Computer, der die Einheit verwenden will, durch Verbindungen zu der Einheit oder durch die Einheit verursacht werden.

Wenn ein Problem mit dem SAN festgestellt wird, stellen Sie immer die Frage „Wurden Änderungen vorgenommen?" Jede Art von Änderung kann fehlerverdächtig sein, vom Computer, der die Einheit verwenden will, bis hin zur Einheit selbst. Dies gilt besonders dann, wenn die Einheit vor einer bestimmten Änderung funktioniert hat, dann aber nach der Änderung nicht mehr funktioniert hat.

Um besser zu verstehen, wie Probleme mit einem SAN diagnostiziert werden können, lesen Sie die folgenden Informationen zur Terminologie und zu typischen Abkürzungen:

Fibre Channel
Fibre Channel gibt eine Glasfaserverbindung zu einer Einheit oder Komponente an.

Hostbusadapter
Ein Hostbusadapter (HBA) wird von einem bestimmten Computer für den Zugriff auf ein SAN verwendet. Die Funktionsweise eines HBA ähnelt insofern der Funktionsweise eines Netzadapters, wie der Zugriff für einen Computer auf ein LAN (lokales Netz) oder WAN (Weitverkehrsnetz) bereitgestellt wird.

SAN Ein SAN ist ein Netz mit gemeinsam genutzten Einheiten, auf die norma-

lerweise über Fibre Channel zugegriffen wird. Oft wird ein SAN verwendet, um Einheiten zwischen vielen verschiedenen Computern gemeinsam zu nutzen.

Hinweise zur SAN-Konfiguration

In SAN-Umgebungen ist es wichtig, dass Sie die SAN-Konfiguration kennen. In verschiedenen SAN-Implementierungen gibt es Einschränkungen und Anforderungen bei der Konfiguration und Einstellung der Einheiten.

Die drei SAN-Konfigurationen sind Punkt-zu-Punkt, Arbitrated Loop und Switched Fabric.

Punkt-zu-Punkt
Die Einheiten sind direkt mit dem Hostbusadapter (HBA) verbunden.

Arbitrated Loop
Arbitrated Loop-Topologien sind Ringtopologien, die bezüglich der Anzahl Einheiten, die in der Ringleitung unterstützt werden, und der Anzahl Einheiten, die jeweils im Gebrauch sein können, beschränkt sind. In einem Arbitrated Loop können nur zwei Einheiten gleichzeitig kommunizieren. Daten, die von einer Einheit gelesen oder auf eine Einheit geschrieben werden, werden von einer Einheit in der Ringleitung an eine andere übergeben, bis sie die Zieleinheit erreichen. Die wichtigste Einschränkung in einem Arbitrated Loop besteht darin, dass nur jeweils zwei Einheiten verwendet werden können.

Switched Fabric
In einem Switched Fabric-SAN sind alle Einheiten in dem Fabric native Fibre-Channel-Einheiten. Diese Topologie hat die größte Bandbreite und Flexibilität, weil alle Einheiten allen HBAs über eine Fibre-Channel-Verbindung zur Verfügung stehen.

Sicherstellen, dass Ihr Hostbusadapter mit Ihrem Speicherbereichsnetz arbeiten kann

Der Hostbusadapter (HBA) ist eine kritische Einheit für die ordnungsgemäße Funktionsweise eines Speicherbereichsnetzes (SAN). Die Probleme, die mit Hostbusadaptern auftreten können, reichen von einer falschen Konfiguration bis zu veraltetem BIOS oder veralteten Einheitentreibern.

Überprüfen Sie für einen bestimmten HBA die folgenden Elemente:

BIOS Hostbusadapter haben ein integriertes BIOS, das aktualisiert werden kann. Der Hersteller des HBA verfügt über Dienstprogramme zum Aktualisieren des BIOS im HBA. Die in Ihrem SAN verwendeten Hostbusadapter sollten regelmäßig überprüft werden, um zu bestimmen, ob BIOS-Updates vorhanden sind, die angewendet werden sollten.

Einheitentreiber
Hostbusadapter verwenden Einheitentreiber zum Arbeiten mit dem Betriebssystem, um Konnektivität mit dem SAN bereitzustellen. Der Hersteller stellt normalerweise einen Einheitentreiber für die Verwendung mit Ihrem HBA zur Verfügung. Außerdem stellt der Hersteller Anweisungen und alle erforderlichen Tools oder Dienstprogramme zum Aktualisieren des Einheitentreibers bereit. Die Version des Einheitentreibers sollte regelmäßig mit der Version verglichen werden, die beim Hersteller verfügbar ist, und bei Bedarf aktualisiert werden, damit die neuesten Fixes und der aktuelle Support berücksichtigt werden.

Konfiguration

Hostbusadapter haben eine Reihe von konfigurierbaren Einstellungen. Die Einstellungen haben normalerweise Einfluss darauf, wie IBM Spectrum Protect mit einer SAN-Einheit arbeitet.

Zugehörige Verweise:

„HBA-Konfigurationsprobleme”

HBA-Konfigurationsprobleme

Hostbusadapter (HBA) haben viele verschiedene Konfigurationseinstellungen und -optionen.

Der HBA-Hersteller stellt normalerweise Informationen zu den Einstellungen für Ihren HBA und die entsprechenden Werte für diese Einstellungen bereit. Außerdem stellt der HBA-Hersteller möglicherweise ein Dienstprogramm und weitere Anweisungen zur Konfiguration Ihres HBA bereit. Die folgenden Einstellungen haben normalerweise Einfluss auf die Verwendung von IBM Spectrum Protect mit einem Speicherbereichsnetz:

- Topologie des Speicherbereichsnetzes (SAN)

  Der HBA muss auf der Basis der gegenwärtig verwendeten SAN-Topologie konfiguriert werden. Ist Ihr SAN beispielsweise ein Arbitrated Loop, muss der HBA für diese Konfiguration definiert werden. Wenn der HBA an einen Switch angeschlossen wird, muss dieser HBA-Anschluss auf „Punkt-zu-Punkt” und nicht auf „Loop” gesetzt werden.

  Mit der SAN-Einheitenzuordnung in IBM Spectrum Protect können Sie eine SAN-Erkennung auf den meisten Systemen ausführen und die persistente Bindung der Einheiten ist nicht erforderlich. Ein IBM Spectrum Protect-Server kann die Einheit finden, wenn der Einheitenpfad aufgrund eines Neustarts oder aus einem anderen Grund geändert wurde.

  Rufen Sie das Support-Portal auf, um die unterstützte Version der Plattform, des Hostbusadapters und des Treibers für die SAN-Erkennung in IBM Spectrum Protect zu überprüfen.

- Fibre-Channel-Verbindungsgeschwindigkeit

  In vielen SAN-Topologien wird das SAN mit einer maximalen Geschwindigkeit konfiguriert. Ist die maximale Fibre-Channel-Switch-Geschwindigkeit beispielsweise 1 GB/Sek, muss der HBA ebenfalls auf diesen Wert gesetzt werden. Andernfalls muss der HBA auf die automatische Festlegung (AUTO) gesetzt werden, wenn der HBA diese Funktion unterstützt.

- Ist Fibre-Channel-Bandunterstützung aktiviert?

  IBM Spectrum Protect erfordert es, dass ein HBA mit Bandunterstützung konfiguriert ist. IBM Spectrum Protect verwendet normalerweise Speicherbereichsnetze für den Zugriff auf Bandlaufwerke und -archive. Daher muss die HBA-Einstellung für die Unterstützung von Bändern aktiviert sein.

AIX Linux Bei der Fehlerbestimmung kann Sie das Modul `dsmsanlist` unterstützen, mit dem Sie Informationen zu Einheiten in einem SAN abrufen können. Das Modul `dsmsanlist` wird bei der Installation des IBM Spectrum Protect-Servers oder des IBM Spectrum Protect-Speicheragenten standardmäßig installiert.

Probleme mit Fibre-Channel-Switchkonfiguration

Ein Fibre-Channel-Switch unterstützt viele verschiedene Konfigurationen. Die Anschlüsse an dem Switch müssen für den Typ des Speicherbereichsnetzes (SAN), das eingerichtet wird, und für die Attribute des SAN entsprechend konfiguriert werden.

Der Hersteller des Switch stellt normalerweise Informationen zu den entsprechenden Einstellungen und zur Konfiguration auf der Basis der SAN-Topologie bereit, die implementiert wird. Außerdem sollte der Switchhersteller ein Dienstprogramm und weitere Anweisungen zur Konfiguration bereitstellen. Die folgenden Einstellungen haben normalerweise Einfluss darauf, wie IBM Spectrum Protect ein Speicherbereichsnetz mit einem Switch verwendet:

Fibre-Channel-Verbindungsgeschwindigkeit
In vielen SAN-Topologien wird das SAN mit einer maximalen Geschwindigkeit konfiguriert. Ist die maximale Fibre-Channel-Switch-Geschwindigkeit beispielsweise 1 GB/Sek, sollte der Hostbusadapter (HBA) ebenfalls auf diesen Wert gesetzt werden. Andernfalls sollte der HBA auf die automatische Festlegung (AUTO) gesetzt werden, wenn der HBA diese Funktion unterstützt.

Anschlussmodus
Die Anschlüsse an dem Switch müssen für den Typ der SAN-Topologie, die implementiert wird, entsprechend konfiguriert werden. Ist das SAN beispielsweise ein Arbitrated Loop, sollte der Anschluss auf FL_PORT gesetzt werden. Wenn in einem anderen Beispiel der HBA an einen Switch angeschlossen wird, sollten die HBA-Optionen auf „Punkt-zu-Punkt" und nicht „Loop" gesetzt werden.

Anschlusseinstellungen für das Datengateway

Ein Datengateway in einem Speicherbereichsnetz (SAN) setzt Fibre-Channel für SCSI-Einheiten, die an das Gateway angeschlossen sind, in SCSI um.

Datengateways werden in Speicherbereichsnetzen vielfach eingesetzt, da sie die Verwendung von SCSI-Einheiten ermöglichen; daher muss sichergestellt werden, dass die Anschlusseinstellungen für ein Datengateway korrekt sind.

Der Anbieter des Datengateways stellt normalerweise Informationen zu den geeigneten Einstellungen und der geeigneten Konfiguration auf der Basis der SAN-Topologie, die implementiert wird, und auf der Basis der verwendeten SCSI-Einheiten bereit. Außerdem stellt der Anbieter möglicherweise ein Dienstprogramm und weitere Anweisungen zur Konfiguration bereit. Die folgenden Einstellungen können für den Fibre-Channel-Anschlussmodus für den verbundenen Anschluss in einem Datengateway verwendet werden:

Private target (privates Ziel)
Nur die SCSI-Einheiten, die an das Datengateway angeschlossen sind, sind über diesen Anschluss sichtbar und verwendbar. Für die verfügbaren SCSI-Einheiten übergibt das Gateway die Rahmen einfach an eine bestimmte Zieleinheit. Anschlusseinstellungen für das private Ziel werden in der Regel für Arbitrated Loops verwendet.

Private target and initiator (privates Ziel und Initiator)
Nur die SCSI-Einheiten, die an das Datengateway angeschlossen sind, sind über diesen Anschluss sichtbar und verwendbar. Für die verfügbaren SCSI-Einheiten übergibt das Gateway die Rahmen einfach an eine bestimmte Zieleinheit. Als Initiator kann dieses Datengateway auch Operationen zum Versetzen von Daten einleiten und verwalten. Es sind erweiterte SCSI-Be-

fehle verfügbar, die eine anbieterspezifische Datenversetzung ermöglichen. Indem ein bestimmter Anschluss als Initiator festgelegt wird, ist er für die Verwendung von SCSI-Anforderungen für die anbieterspezifische Datenversetzung auswählbar.

Public target (öffentliches Ziel)
Alle SCSI-Einheiten, die an das Datengateway angeschlossen sind, sowie andere von der Struktur verfügbare Einheiten sind über diesen Anschluss sichtbar und verwendbar.

Public target and initiator (öffentliches Ziel und Initiator)
Alle SCSI-Einheiten, die an das Datengateway angeschlossen sind, sowie andere von der Struktur verfügbare Einheiten sind über diesen Anschluss sichtbar und verwendbar. Als Initiator kann dieses Datengateway auch Operationen zum Versetzen von Daten einleiten und verwalten. Es sind erweiterte SCSI-Befehle verfügbar, die eine anbieterspezifische Datenversetzung ermöglichen. Indem ein bestimmter Anschluss als Initiator festgelegt wird, ist er für die Verwendung von SCSI-Anforderungen für die anbieterspezifische Datenversetzung auswählbar.

SAN-Konfiguration zwischen Einheiten

Einheiten in einem Speicherbereichsnetz (SAN), wie z. B. ein Datengateway oder ein Switch, stellen in der Regel Dienstprogramme bereit, die anzeigen, welche Informationen diese Einheit im SAN sieht.

Diese Dienstprogramme dienen zum besseren Verständnis der Konfiguration Ihres SAN und erleichtern die Behebung von Fehlern in der Konfiguration. Der Anbieter des Datengateways oder Switchs stellt in der Regel ein Dienstprogramm für die Konfiguration bereit. Im Rahmen dieses Konfigurationsdienstprogramms werden normalerweise Informationen wie beispielsweise Folgende verwendet:

- Typ der Konfiguration für die Einheit
- Andere für diese Einheit erkennbare Informationen in der SAN-Topologie (zu der sie gehört)

Sie können diese Dienstprogramme anderer Anbieter zum Überprüfen der SAN-Konfiguration zwischen Einheiten verwenden:

Datengateway
Ein Datengateway meldet alle Fibre-Channel-Einheiten und die SCSI-Einheiten zurück, die in dem SAN verfügbar sind.

Switch
Ein Switch meldet Informationen zur SAN-Struktur zurück.

Fibre-Channel-Verbindungsfehlerbericht

Die meisten SAN-Einheiten stellen Überwachungstools bereit, die verwendet werden können, um Informationen zu Fehlern und zur Leistungsstatistik zurückzumelden.

Der Hersteller der Einheit sollte ein Dienstprogramm für die Überwachung bereitstellen. Wenn ein Überwachungstool verfügbar ist, meldet es normalerweise Fehler zurück. Die folgenden Fehler treten häufiger auf:

CRC-Fehler, 8b/10b-Codefehler und andere ähnliche Symptome
Diese Fehler sind behebbar, wobei die Fehlerbehandlung normalerweise von der Firmware oder Hardware bereitgestellt wird. In den meisten Fällen besteht die Methode zur Wiederherstellung der Einheit darin, den fehlerhaften Frame erneut zu übertragen. Die Fibre-Channel-Verbindung ist noch aktiv, wenn diese Fehler festgestellt werden. Anwendungen, die eine SAN-

Einheit verwenden, auf der dieser Typ von Verbindungsfehler auftritt, ist normalerweise der Fehler nicht bekannt, es sei denn, es handelt sich um einen schwer wiegenden Fehler. Ein schwer wiegender Fehler ist ein Fehler, bei dem die Wiederherstellung durch die Firmware und Hardware die Daten nach wiederholten Versuchen nicht erfolgreich erneut übertragen kann. Die Wiederherstellung für diese Fehlertypen erfolgt normalerweise sehr schnell und hat keine Verminderung der Systemleistung zur Folge.

Verbindungsfehler (Verlust des Signals, Verlust der Synchronisation, NOS-Basiselement empfangen)

Dieser Fehler gibt an, dass eine Verbindung für einen Zeitraum tatsächlich „unterbrochen" ist. Der Fehler wird wahrscheinlich durch einen fehlerhaften Gigabit Interface Converter, fehlerhaften Media Interface Adapter (MIA) oder ein fehlerhaftes Kabel verursacht. Die Wiederherstellung für diesen Typ von Fehler ist mit Unterbrechungen verbunden. Dieser Fehler wird in der Anwendung angezeigt, die die SAN-Einheit verwendet, auf der dieser Verbindungsfehler festgestellt wurde. Die Wiederherstellung erfolgt auf der Befehlsaustauschebene und beinhaltet, dass die Anwendung und der Einheitentreiber eine Zurücksetzung für die Firmware und Hardware ausführen müssen, was zu einer Verminderung der Systemleistung führt, bis die Wiederherstellung der Verbindung abgeschlossen ist. Diese Fehler sollten genau überwacht werden, da sie normalerweise mehrere SAN-Einheiten betreffen.

Hinweis: Fibre-Channel-Verbindungsfehler werden oft durch eine Aktion zum Austauschen einer SAN-Einheit durch den Kundendienst verursacht. Im Rahmen der Wartung, die vom Kundendienst zum Austauschen oder Reparieren einer SAN-Einheit ausgeführt wird, kann das Fibre-Channel-Kabel vorübergehend getrennt sein. Ist dies der Fall, sollten Zeitpunkt und Dauer des Fehlers der Zeit entsprechen, zu der die Serviceaktivität ausgeführt wurde.

Allgemeine SAN-Einheitenfehler

Verschiedene SAN-spezifische Nachrichten können ausgegeben werden, wenn Probleme mit Ihren SAN-Einheiten des Speicheragenten auftreten.

Tabelle 16 enthält Fehler, die für SAN-Einheiten generiert werden.

Tabelle 16. Allgemeine SAN-Einheitenfehler

Fehler	Erläuterung
ANR8302E E/A-Fehler in Laufwerk *TSMDRIVE01* (*/dev/mt9*) (OP=*WRITE*, Fehlernummer=*5*, CC=*205*, KEY=*FF*, ASC=*FF*, ASCQ=*FF*, SENSE=**NONE**, Beschreibung=*Allgemeiner SCSI-Fehler*). Die entsprechende Maßnahme ist in Anhang D des Nachrichtenhandbuchs angegeben.	Diese Nachricht wird oft für SAN-Einheitenfehler ausgegeben. CC=205 gibt an, dass der Einheitentreiber einen SCSI-Adapterfehler erkennt. Falls eine an ein SAN angeschlossene Einheit das Zurücksetzen einer Verbindung aufgrund eines Verbindungsverlustes feststellt, wird dies an den Einheitentreiber als SCSI-Adapterfehler zurückgemeldet. Die zu Grunde liegende Ursache dieses Fehlers ist das Ereignis, das das Zurücksetzen der Verbindung aufgrund des Verbindungsverlustes verursacht hat. Der Pfad für diese Einheit könnte mit ONLINE=NO aktualisiert werden, indem der Befehl **`UPDATE PATH`** ausgegeben wird. Setzen Sie den Pfad erst auf ONLINE=YES, wenn die Ursache für das Zurücksetzen der Verbindung isoliert und korrigiert wurde.

Tabelle 16. Allgemeine SAN-Einheitenfehler (Forts.)

Fehler	Erläuterung
ANR8957E: *Befehl*: Autodetect ist OFF, und die von dem Kassettenarchiv gemeldete Seriennummer stimmt nicht mit der Seriennummer in der Kassettenarchivdefinition überein.	Die SAN-Einheitenzuordnung in IBM Spectrum Protect hat einen Pfad für das Kassettenarchiv entdeckt, der eine andere Seriennummer als die aktuelle IBM Spectrum Protect-Definition für das Kassettenarchiv zurückmeldet. Der Parameter **AUTODETECT** für den Befehl war auf NO gesetzt. Dadurch wurde die Aktualisierung der Seriennummer für das Kassettenarchiv durch den Server verhindert. Bestimmen Sie den neuen Pfad und geben Sie den Befehl **UPDATE PATH** aus, um diesen Fehler zu korrigieren.
ANR8958E: *Befehl*: Autodetect ist OFF, und die von dem Laufwerk gemeldete Seriennummer stimmt nicht mit der Seriennummer in der Laufwerkdefinition überein.	Die SAN-Einheitenzuordnung in IBM Spectrum Protect hat einen Pfad für ein Laufwerk entdeckt, der eine andere Seriennummer als die aktuelle IBM Spectrum Protect-Definition für dieses Laufwerk zurückmeldet. Der Parameter AUTODETECT für den Befehl war auf NO gesetzt. Dadurch wurde die Aktualisierung der Seriennummer für dieses Laufwerk durch den Server verhindert. Bestimmen Sie den neuen Pfad und geben Sie den Befehl **UPDATE PATH** aus, um diesen Fehler zu korrigieren.

Tabelle 16. Allgemeine SAN-Einheitenfehler (Forts.)

Fehler	Erläuterung
ANR8963E: Pfad kann nicht gefunden werden, um die für Laufwerk *Laufwerkname* in Kassettenarchiv *Kassettenarchivname* definierte Seriennummer abzugleichen.	Die SAN-Einheitenzuordnung konnte eine SAN-Einheit nicht finden, die zuvor für den Server definiert wurde. Die wahrscheinlichste Ursache ist, dass die Einheit selbst entfernt oder im SAN ersetzt wurde. Die folgenden Schritte können diesen Fehler beheben: • Einheit entfernt Wurde die Einheit aus dem SAN entfernt, löschen Sie die Serverdefinitionen, die auf diese Einheit verweisen. Geben Sie den Befehl `QUERY PATH F=D` aus, um alle Pfade zu bestimmen, die auf die Einheit verweisen. Geben Sie dann den Befehl **`DELETE PATH`** aus, um diese Pfade zu entfernen. • Einheit ersetzt Eine SAN-Einheit wurde aufgrund einer Wartung oder eines Upgrades durch eine neue Einheit ersetzt. Führen Sie die folgenden Prozeduren aus: – Versuchen Sie, die Laufwerk- oder Laufwerkpfaddefinition nach dem Ersetzen des Laufwerks nicht zu löschen. – Geben Sie einen der folgenden Serverbefehle aus: - `UPDate DRive <Kassettenarchivname> <Laufwerkname> SERIAL=AUTODetect` Dieser Befehl erzwingt die Aufzeichnung der neuen Seriennummer in der Serverdatenbank. Da das Laufwerk ersetzt wird, bleibt die Elementnummer identisch. - `UPDate PATH <Quellenname> <Laufwerkname> SRCT=SERVER DESTT=DRIVE LIBRary=<Kassettenarchivname> DEVIce=xxxxx AUTODetect=Yes` Dieser Befehl erzwingt die Aufzeichnung der neuen Seriennummer in der Datenbank. Da das Laufwerk ersetzt wird, bleibt die Elementnummer identisch. – Wenn das Laufwerk oder der Laufwerkpfad gelöscht wird, definieren Sie dieses neue, ersetzte Laufwerk erneut. Sie müssen den IBM Spectrum Protect-Server erneut starten, damit die Zuordnung der Elementnummer und Seriennummer für das Kassettenarchiv aktualisiert wird. Diese Zuordnung erfolgt nur bei der Initialisierung. Geben Sie den Befehl **`QUERY PATH F=D`** aus, um alle auf dem Server definierten Pfade zu suchen, die auf diese Einheit verweisen. Geben Sie dann den folgenden Befehl aus, um die Pfadinformationen zu aktualisieren: `UPDATE PATH AUTODetect=Yes`

Tabelle 16. Allgemeine SAN-Einheitenfehler (Forts.)

Fehler	Erläuterung
ANR8972E: Die Elementnummer für Laufwerk *Laufwerkname* in Kassettenarchiv *Kassettenarchivname* kann nicht gefunden werden.	Wenn der Parameter **ELEMent** beim Definieren des Laufwerks auf AUTODetect gesetzt wird, ruft IBM Spectrum Protect automatisch die Elementnummer des Laufwerks ab. Wenn das Kassettenarchiv jedoch keine Zuordnung der Elementnummer und Seriennummer bereitstellt, wird diese Nachricht ausgegeben. Führen Sie die folgenden Schritte aus, um diesen Fehler zu korrigieren: 1. Bestimmen Sie die Elementnummer für dieses Bandlaufwerk. 2. Geben Sie den Befehl **UPDATE DRIVE** aus, um die Elementnummer der Einheit zu aktualisieren.

AIX Linux Bei der Fehlerbestimmung kann Sie das Modul `dsmsanlist` unterstützen, mit dem Sie Informationen zu Einheiten in einem SAN abrufen können. Das Modul `dsmsanlist` wird bei der Installation des IBM Spectrum Protect-Servers oder des IBM Spectrum Protect-Speicheragenten standardmäßig installiert.

Zugehörige Konzepte:

„Fehler bei der SAN-Einheitenzuordnung" auf Seite 200

Hinweise und Tipps zur SAN-Einheitenzuordnung

Die SAN-Einheitenerkennung und -Einheitenzuordnung werden unter Windows, AIX und Linux (außer Linux zSeries) unterstützt.

Nachfolgend werden die Vorteile der SAN-Einheitenerkennung und -Einheitenzuordnung in IBM Spectrum Protect erläutert:

IBM Spectrum Protect kann alle Einheiten im Speicherbereichsnetz (SAN) anzeigen
Mit dem Serverbefehl **QUERY SAN** werden alle Einheiten angezeigt, die vom Server über alle auf dem System installierten Fibre Channel-Hostbusadapter erkannt werden. Die angezeigten Parameter sind Einheitentyp, Herstellername, Name des Produktmodells, Seriennummer und Einheitenname. Wird in der Abfrage `FORMAT=DETAIL` angegeben, werden weitere Informationen, wie z. B. weltweiter Name, Anschluss, Bus, Ziel und LUN, angezeigt. Mit diesen Informationen können alle Bandeinheiten, Platteneinheiten und Einheiten zum Versetzen von Daten in dem Speicherbereichsnetz identifiziert werden. Für AIX ist die Einheit zum Versetzen von Daten nicht erkennbar und wird nicht angezeigt.

IBM Spectrum Protect kann den Einheitenpfad automatisch aktualisieren, wenn sich der Pfad einer Einheit ändert
IBM Spectrum Protect erfordert keine persistente Bindung für die Einheiten, die über den Hostbusadapter (HBA) erkannt werden. Stattdessen verwendet der Server die SNIA (Storage Networking Industry Association) HBAAPI, um die Seriennummer für alle Einheiten in dem SAN zu erkennen und abzurufen. Er kann auch den Pfad jeder Einheit bestimmen. Durch den Vergleich der Seriennummer einer Einheit, die in der IBM Spectrum Protect-Datenbank aufgezeichnet ist, mit der Seriennummer, die in Echtzeit von der Einheit abgerufen wird, wird eine Änderung am Pfad einer Einheit erkannt. Wenn der Pfad geändert wurde, ruft die SAN-Erkennung automatisch den neuen Pfad für die Einheit ab. Die IBM Spectrum Protect-Datenbank wird ebenfalls mit den neuen Pfadangaben aktualisiert.

Die HBAAPI-Wrapperbibliothek ist der Wrapper, der vom Server verwendet wird, um mit der SNIA HBAAPI zu kommunizieren. Die HBAAPI-Wrapperbibliothek wird in demselben Verzeichnis wie die ausführbare IBM Spectrum Protect-Datei installiert (es sei denn, der vollständige Pfad wird angegeben). Die folgende Liste zeigt die HBA-Wrapperdateien, die im Serverpaket enthalten sind (außer unter AIX):

- Windows `hbaapi.dll`
- AIX `/usr/lib/libhbaapi.a` (von AIX mit HBAAPI-Installation bereitgestellt)
- Linux 32-Bit: `libhbaapi32.so`
- Linux 64-Bit: `libhbaapi64.so`

Wenn eine dieser Dateien fehlt, wird die Nachricht „ANR1791W Die HBAAPI-Wrapperbibliothek xxxxxxxxx konnte nicht geladen werden oder die Wrapperbibliothek ist nicht vorhanden" angezeigt.

SAN-Einheitenzuordnung inaktivieren:

Gelegentlich müssen Sie die SAN-Einheitenzuordnung inaktivieren, um ein Problem zu umgehen oder einzugrenzen, wenn Sie Probleme mit Einheiten beheben.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die SAN-Einheitenzuordnung und die SAN-Einheitenerkennung zu inaktivieren:

Vorgehensweise

Geben Sie den Serverbefehl **setopt SANDISCOVERY OFF** aus. Die Befehle **setopt SANDISCOVERY** können so oft wie erforderlich ausgegeben werden.

Tipp: Die SAN-Erkennung kann auch inaktiviert/aktiviert werden, indem die folgende Option in die Datei `dsmserv.opt` eingegeben wird:

SANDISCOVERY OFF - Mit dieser Option wird die SAN-Erkennung inaktiviert.

SANDISCOVERY ON - Mit dieser Option wird die SAN-Erkennung aktiviert.

SANDISCOVERY ON ist der Standardwert für die AIX-, Linux- und Windows-Plattformen.

Plattformspezifische Informationen:

Wenn Sie Ihre SAN-Einheitenzuordnung bearbeiten, ist es wichtig, dass Sie die plattformspezifischen Informationen kennen.

AIX Mit dem Befehl **QUERY SAN** werden keine Gateway-Einheiten angezeigt, da Gateway-Einheiten für AIX nicht sichtbar sind.

Linux Es gibt separate Bibliotheken, Dienstprogramme und andere Elemente für RHEL3U3. Um diese auszuführen, müssen Sie zusätzlich zum Emulex-Treiber auch ein Emulex-ioctl-Kernelmodul installieren. Stellen Sie sicher, dass Sie den Emulex-Treiber laden, bevor Sie das ioctl-Modul laden.

Tipp: Siehe die Liste der unterstützten HBAs und der erforderlichen Treiberversionen nach Betriebssystem.

Fehler bei der SAN-Einheitenzuordnung

Die Fehler, die während der SAN-Einheitenzuordnung am häufigsten generiert werden, beziehen sich auf die SAN-Erkennung, auf Störungen bei SAN-Einheiten, auf ungültige Kassettenarchive und auf andere SAN-bezogene Probleme.

ANR1745I: SAN-Einheiten können nicht erkannt werden. Funktion ist aktiv.

Diese Fehlernachricht wird angezeigt, wenn eine andere aktive SAN-Erkennung vorhanden ist.

Der Server kann keine SAN-Erkennung ausführen. Wiederholen Sie die Anforderung, nachdem die andere SAN-Erkennung abgeschlossen wurde.

ANR1786W, ANR1787W oder ANR1788W

Möglicherweise werden die Fehlernachrichten ANR1786W, ANR1787W und ANR1788W bei einem Problem mit der SAN-Erkennung angezeigt. Die folgenden drei Nachrichten geben normalerweise an, dass die HBAAPI-Bibliothek im Allgemeinen nicht arbeitet:

- ANR1786W HBAAPI kann den Adapternamen nicht abrufen.
- ANR1787W Adapter *Adaptername* kann nicht geöffnet werden.
- ANR1788W Adapterattribute für *Adaptername* können nicht abgerufen werden.

Kann der Server als Ergebnis keine SAN-Erkennung ausführen, rufen Sie das Support Portal auf, um zu überprüfen, ob der Treiber für den Hostbusadapter aktuell ist und eine unterstützte Version hat.

ANR1789W Abrufen der HBA-Zielzuordnung ist fehlgeschlagen

Die Fehlernachricht ANR1789W bezieht sich auf den häufigsten HBAAPIn-Fehler im SAN.

„Abrufen der HBA-Zielzuordnung ist fehlgeschlagen" bedeutet, dass der Hostbusadapter beim Zusammenstellen von Informationen zur Einheitenzuordnung durch Senden verschiedener SCSI-Befehle einen Fehler festgestellt hat.

Stellen Sie sicher, dass alle SAN-Einheiten ordnungsgemäß arbeiten (z. B. ist möglicherweise ein SAN-Datengateway blockiert, für das eventuell ein Warmstart durchgeführt werden muss). Sind alle Einheiten funktionsbereit, stellen Sie sicher, dass die Firmware der Einheit im SAN und der Treiber für den Hostbusadapter die entsprechenden Versionen haben. Kann der Server als Ergebnis keine SAN-Erkennung ausführen, rufen Sie das Support Portal auf, um zu überprüfen, ob der Treiber für den Hostbusadapter aktuell ist und eine unterstützte Version hat.

Tipp: Stellen Sie für IBM Bandeinheiten sicher, dass die neueste Firmware installiert ist. Firmware vor 4772 für Bandeinheiten IBM 3580 verursacht Probleme mit Qlogic HBAAPI.

ANR1790W Die SAN-Erkennung ist fehlgeschlagen

Die Fehlernachricht ANR1790W ist eine allgemeine Nachricht, die angibt, dass die HBAAPI-Funktion fehlgeschlagen ist und die SAN-Erkennung nicht ausführen kann.

Stellen Sie sicher, dass alle SAN-Einheiten ordnungsgemäß arbeiten (z. B. ist möglicherweise ein SAN-Datengateway blockiert, für das eventuell ein Warmstart durchgeführt werden muss). Sind alle Einheiten funktionsbereit, stellen Sie sicher, dass die Firmware der Einheit im SAN und der Treiber für den Hostbusadapter die entsprechenden Versionen haben.

Tipp: Stellen Sie für IBM Bandeinheiten sicher, dass die neueste Firmware installiert ist. Firmware vor 4772 für Bandeinheiten IBM 3580 verursacht Probleme mit Qlogic HBAAPI.

ANR1791W Die HBAAPI-Wrapperbibliothek xxxxx konnte nicht geladen werden oder die Wrapperbibliothek ist nicht vorhanden

Die HBAAPI-Wrapperbibliothek wird vom Server verwendet, um mit der SNIA HBAAPI zu kommunizieren.

Die HBAAPI-Wrapperbibliotheken befinden sich in demselben Verzeichnis wie die ausführbare IBM Spectrum Protect-Datei (es sei denn, der vollständige Pfad ist wie unten gezeigt angegeben). Die folgende Liste zeigt die HBA-Wrapperdateien, die mit dem Serverpaket ausgeliefert werden (mit Ausnahme von AIX und Linux zSeries). Die Fehlernachricht ANR1791W gibt an, dass die HBAAPI-Wrapperdatei entweder fehlt oder von IBM Spectrum Protect möglicherweise nicht geladen werden konnte. Stellen Sie sicher, dass sich die Wrapperdatei in demselben Verzeichnis wie die ausführbare IBM Spectrum Protect-Datei befindet. Die HBAAPI-Wrapperbibliotheksdateien werden in der folgenden Liste gezeigt:

- Windows `hbaapi.dll`
- AIX `/usr/lib/libhbaapi.a` (von AIX mit HBAAPI-Installation bereitgestellt)
- Linux 32-Bit: `libhbaapi32.so`
- Linux 64-Bit: `libhbaapi64.so`

Das Ergebnis ist, dass der Server keine SAN-Erkennung ausführen kann.

ANR1792W Die HBAAPI-Lieferantenbibliothek konnte nicht geladen werden oder die Lieferantenbibliothek ist nicht vorhanden

Die Fehlernachricht ANR1792W gibt an, dass die Bibliotheksdatei des Lieferanten nicht geladen werden konnte. Überprüfen Sie die Gültigkeit der Bibliotheksdateien.

AIX- oder Linux-Systeme (außer Linux zSeries) speichern ihre HBAAPI-Bibliotheken an der Position, die von der Datei `/etc/hba.conf` angegeben wird. Windows-Dateien werden im Verzeichnis `C:\winnt\system32` gespeichert. Die folgenden Beispiele zeigen Lieferantenbibliotheksdateien:

- `C:\winnt\system32\qlsdm.dll` (QlLogic Windows-Datei)
- `/usr/lib/libHBAAPI.a` (Emulex AIX-Datei)
- `/usr/lib/libqlsdm.so` (Qlogic Linux-Datei)
- `/usr/lib/libemulexhbaapi.so` (Emulex Linux 32-Bit-Datei)
- `/usr/lib64/libemulexhbaapi.so` (Emulex Linux 64-Bit-Datei)

Das Ergebnis ist, dass der Server keine SAN-Erkennung ausführen kann.

ANR1793W Die IBM Spectrum Protect SAN-Erkennung wird auf dieser Plattform oder unter dieser Version des Betriebssystems nicht unterstützt

Die Fehlernachricht ANR1793W wird nur angezeigt, wenn IBM Spectrum Protect versucht, eine Operation für die SAN-Einheitenzuordnung oder -Einheitenerkennung auf einem nicht unterstützten Betriebssystem auszuführen. Die folgenden Betriebssysteme werden gegenwärtig nicht von der SAN-Einheitenzuordnung oder -Einheitenerkennung unterstützt:

- 64-Bit Windows 2003
- AIX-Versionen, die nicht 52L oder 53A sind. Die Unterstützung für die SAN-Einheitenzuordnung und -Einheitenerkennung unter AIX erfordert entweder Version 52L (Dateigruppenstufe 5.2.0.50) oder 53A (Dateigruppenstufe 5.3.0.10) oder höher.

Das Ergebnis ist, dass der Server keine SAN-Erkennung ausführen kann.

ANR1794W Die IBM Spectrum Protect SAN-Erkennung ist durch Optionen inaktiviert

Die Fehlernachricht ANR1794W gibt an, dass die SAN-Erkennung auf dem Server inaktiviert ist.

Die SAN-Erkennung kann mit den folgenden Serverbefehlen inaktiviert oder aktiviert werden:

setopt SANDISCOVERY OFF und setopt SANDISCOVERY PASSIVE
Mit diesen beiden Befehlen wird die SAN-Erkennung inaktiviert. Der Server kann den Einheitenpfad nicht automatisch korrigieren, wenn der Pfad geändert wurde. Dieser Befehl muss nur einmal ausgegeben werden.

Der Unterschied zwischen den beiden Befehlen ist der, dass **SANDISCOVERY OFF** die Einheit aufruft und den inaktiven Pfad als offline markiert. **SANDISCOVERY PASSIVE** ruft die Einheit nicht auf und markiert den inaktiven Pfad nicht als offline.

setopt SANDISCOVERY ON
Mit diesem Befehl wird die SAN-Erkennung aktiviert. Der Befehl **SETOPT SANDISCOVERY ON** kann beliebig oft ausgegeben werden.

Die SAN-Erkennung kann auch inaktiviert/aktiviert werden, indem die folgende Option in die Datei `dsmserv.opt` eingefügt wird:

SANDISCOVERY OFF oder SANDISCOVERY PASSIVE
Mit diesen beiden Befehlen kann die SAN-Erkennung inaktiviert werden.

SANDISCOVERY ON
Mit diesem Befehl wird die SAN-Erkennung aktiviert.

Für AIX Linux Windows **SANDISCOVERY** gilt die Standardeinstellung ON.

Rufen Sie das Support Portal auf, um die unterstützte Version der Plattform, des Hostbusadapters und des Treibers zu überprüfen, bevor die Einstellung **SANDISCOVERY** ON zum Aktivieren der SAN-Erkennung definiert wird.

AIX Linux Bei der Fehlerbestimmung kann Sie das Modul `dsmsanlist` unterstützen, mit dem Sie Informationen zu Einheiten in einem SAN abrufen kön-

nen. Das Modul `dsmsanlist` wird bei der Installation des Servers oder des Speicheragenten standardmäßig installiert.

ANR2034E QUERY SAN: Keine Übereinstimmung für diese Kriterien gefunden

Die Fehlernachricht ANR2034E wird ausgegeben, wenn der Server versucht, Konfigurationsdaten für das Speicherbereichsnetz (SAN) zu erfassen, aber der Server keine Daten findet.

Das Ergebnis ist, dass der Server keine SAN-Erkennung ausführen kann.

Die folgende Liste enthält mögliche Ursachen, warum keine Informationen zum SAN gefunden werden:

- Das System oder die Betriebssystemversion wird nicht unterstützt.
- Diese Umgebung ist keine SAN-Umgebung.
- Möglicherweise liegt ein Problem mit dem SAN vor.
- HBAAPI gibt möglicherweise den Wert null für die Anzahl der Hostbusadapter (HBA) auf dem System zurück.
- HBAAPI gibt möglicherweise den Wert null für die Anzahl der Einheiten auf dem System zurück.

Führen Sie die folgenden Tasks aus, um die SAN-Konfigurationsdaten zu finden:

- Überprüfen Sie den Fibre-Channel-HBA-Treiber und stellen Sie sicher, dass er installiert und aktiviert ist.
- Überprüfen Sie die HBA-Treiberversion, um sicherzustellen, dass sie aktuell ist.
- Verwenden Sie das Dienstprogramm des HBA-Lieferanten, um zu überprüfen, ob Fibre-Channel-Verbindungsprobleme zurückgemeldet wurden.
- Deinstallieren Sie den HBA-Treiber und installieren Sie ihn erneut. Liegt ein Problem mit der HBA-Konfiguration, dem Einheitentreiber oder der Kompatibilität vor, kann die Deinstallation und die erneute Installation manchmal das Problem beheben.
- Überprüfen Sie die Fibre-Channel-Kabelverbindung zum HBA.
- Überprüfen Sie die Fibre-Channel-Kabelverbindung vom HBA zur SAN-Einheit (Switch, Datengateway oder andere Einheit).
- Überprüfen Sie den Gigabit Interface Converter (GBIC).
- Verwenden Sie auf der SAN-Einheit (Switch, Datengateway oder andere Einheit) einen anderen Zielport. Manchmal können die SAN-Einheiten einen bestimmten Portfehler haben.
- Halten Sie den Server an, starten Sie das System erneut und starten Sie den Server erneut. Wurden Konfigurationsänderungen im SAN vorgenommen, erfordern das Betriebssystem, der Einheitentreiber und der Hostbusadapter manchmal einen Neustart des Systems, bevor sie mit dem SAN kommunizieren können.
- Stoppen Sie den Zielport auf der SAN-Einheit und starten Sie ihn erneut.
- Nehmen Sie die HBA-Karte heraus und stecken Sie die Karte wieder ein.
- Ersetzen Sie den HBA.

ANR8226E Fehler beim Ermitteln der Version der HBA-API-Bibliothek

Die Fehlernachricht ANR8226E wird nur für AIX angezeigt.

Der Server hat versucht, die Version der Dateigruppe devices.common.IBM.fc.hba-api zu bestimmen, und hat einen Fehler festgestellt. Die Fehlernachricht ANR8226E gibt an, dass beim Versuch, die Version der HBA-API-Bibliotheksdateigruppe unter AIX zu ermitteln, ein Fehler aufgetreten ist.

Das Ergebnis ist, dass der Server keine SAN-Erkennung ausführen kann.

AIX

ANR8227E Dateigruppe devices.common.IBM.fc.hba-api hat nicht die erforderliche Stufe

Aufgrund von Fehlern im AIX HBAAPI-Code sind die folgenden Mindestversionen der Dateigruppe devices.common.IBM.fc.hba-api für eine erfolgreiche SAN-Erkennung erforderlich:

- AIX52 - Erfordert 5.2.0.50
- AIX53 - Erfordert 5.3.0.10

Der Server hat angegeben, dass die Dateigruppe devices.common.IBM.fc.hba-api eine Version hat, die mit IBM Spectrum Protect-Operationen nicht kompatibel ist. Installieren Sie das neueste Wartungspaket für diese Dateigruppe, wenn Sie SAN-Einheiten verwenden.

Das Ergebnis ist, dass der Server keine SAN-Erkennung ausführen kann.

Zugehörige Verweise:

„Hinweise und Tipps zur SAN-Einheitenzuordnung” auf Seite 198

SAN-Einheiten fehlen in der Anzeige des Serverbefehls QUERY SAN:

Wenn der Serverbefehl **QUERY SAN** nicht alle Einheiten anzeigt, können Probleme mit der Konfiguration oder mit der Herstellerunterstützung die Ursache sein.

Stellen Sie sicher, dass für die Serveroption SANDISCOVERY die Einstellung NO festgelegt ist.

SAN-Konfiguration aktualisieren:

Aufgrund der SAN-Konfiguration zeigt der Serverbefehl **QUERY SAN** möglicherweise nicht alle Einheiten an.

Sie müssen möglicherweise das SAN aktualisieren, da die Konfiguration geändert wurde (Einheit hinzufügen/entfernen) und die Systemkonfiguration aktualisiert werden muss.

Konfiguration unter AIX aktualisieren:

Für IBM Einheiten:

Geben Sie den Befehl **cfgmgr** aus, um neue Einheiten zu konfigurieren und die neue Konfiguration anzuzeigen. Der Gerätedateiname für IBM Bandeinheiten (nicht die IBM Spectrum Protect-Einheiten) ist /dev/rmtX für Bandlaufwerke und /dev/smcX für Datenträgerwechsler.

Tipp: Gerätedateiname: /dev/rmt0, /dev/smc0

Für IBM Spectrum Protect-Einheiten:

Um die Gerätedateien zu aktualisieren, verwenden Sie **smitty** > **Einheiten** > **IBM Spectrum Protect-Einheiten** > **Alle definierten**

Einheiten entfernen und dann **Von IBM Spectrum Protect unterstützte Einheiten erkennen**. Der Gerätedateiname ist /dev/mtX für Bandlaufwerke und /dev/lbX für Datenträgerwechsler.

Tipp: Gerätedateiname: `/dev/mt0, /dev/lb0`

Alternativ können Sie den IBM Einheitentreiber erneut installieren. Der IBM Spectrum Protect-Einheitentreiber aktualisiert alle aktuellen Gerätedateinamen.

Konfiguration unter Windows aktualisieren:

Mit dem Plug and Play wird die Windows-Registry aktualisiert und der Einheitenname kann geändert werden, ohne dass der Computer erneut gestartet oder der Einheitentreiber einbezogen werden muss. Der IBM Spectrum Protect-Server erkennt die Änderung an einem Gerätedateinamen und aktualisiert den neuen Gerätedateinamen, wenn er auf die Bandeinheiten zugreift (während der Serverinitialisierung oder des normalen Betriebs). Der korrekte Einheitenname wird in der IBM Spectrum Protect-Datenbank aktualisiert. Der Gerätedateiname lautet `/dev/mtA.B.C.D` für IBM Spectrum Protect-Einheiten und IBM Einheiten und `/dev/lbA.B.C.C` für IBM Spectrum Protect-Einheiten und IBM Datenträgerwechsler. Der Gerätedateiname TapeX gilt nur für IBM Bandlaufwerke und der Gerätedateiname ChangerX gilt nur für IBM Datenträgerwechsler.

Tipp: Gerätedateiname: `mt0.1.0.0`, `lb0.0.1.0`, `Tape0` und `Changer0`.

Konfiguration unter Linux aktualisieren:

Der Hostbusadapter (HBA) erhält die aktuellen Konfigurationsdaten als Ergebnis des RSCN. Manchmal muss der Computer erneut gestartet werden, damit die Konfigurationsänderungen berücksichtigt werden.

Für IBM Einheiten:

Geben Sie den Befehl **`lin_taped`** aus, um Einheiten zu rekonfigurieren. Die Einheitendaten können für Bandeinheiten aus der Datei `/proc/scsi/IBMtape` und für Datenträgerwechsler aus der Datei `/proc/scsi/IBMchanger` abgerufen werden. Der Gerätedateiname lautet /dev/IBMTapeX für Bandeinheiten und /dev/IBMChangerX für Datenträgerwechsler.

Tipp: Gerätedateiname: `/dev/IBMTape0, /dev/IBMChanger0`

Für IBM Spectrum Protect-Einheiten:

Benutzer können 'autoconf' verwenden, das Script zum automatischen Konfigurieren des IBM Spectrum Protect-Einheitentreibers. Dieses Script muss sich im Verzeichnis `/opt/tivoli/tsm/devices/bin` befinden (oder in demselben Verzeichnis wie die Datei `tsmscsi`), damit Einheiten konfiguriert und alle aktuellen Gerätedateinamen und Einheitendaten abgerufen werden können. Der Gerätedateiname lautet `/dev/mtX` für Bandeinheiten und `/dev/lbX` für Datenträgerwechsler.

Tipp: Gerätedateiname: `dev/tsmscsi/mt0, /dev/tsmscsi/lb0`

Alternativ können Sie den IBM Einheitentreiber erneut installieren. Der IBM Spectrum Protect-Einheitentreiber aktualisiert alle aktuellen Gerätedateinamen.

Mit dem Linux-Durchgriffseinheitentreiber für die IBM Spectrum Protect-Einheiten müssen der HBA-Treiber und der generische Treiber erneut gela-

den werden, um alle aktuellen Gerätedateinamen abzurufen. Sie müssen das Script 'autoconf' ausführen, damit der IBM Spectrum Protect-Einheitentreiber Konfigurationsdateien (`/dev/tsmscsi/lbinfo` und `/dev/tsmscsi/mtinfo`) erstellen kann. Diese Dateien werden vom IBM Spectrum Protect-Server verwendet, um nach jeder SAN-Erkennung die Gerätedateinamen zu erstellen.

32-Bit (Linux xSeries)
Stellen Sie sicher, dass sich die HBAAPI-Wrapperbibliothek libhbaapi32.so in demselben Verzeichnis wie `dsmserv` oder im Verzeichnis `/opt/tivoli/tsm/server/bin` befindet.

64-Bit (Linux pSeries)
Stellen Sie sicher, dass sich die HBAAPI-Wrapperbibliothek `libhbaapi64.so` in demselben Verzeichnis wie `dsmserv` oder im Verzeichnis `/opt/tivoli/tsm/server/bin` befindet.

64-Bit (Linux zSeries)
Stellen Sie sicher, dass sich die Pseudo-HBAAPI-Wrapperbibliothek `libhbaapi64.so` in demselben Verzeichnis wie `dsmserv` oder im Verzeichnis `/opt/tivoli/tsm/server/bin` befindet. Die Wrapperbibliothek `libhbaapi64.so` ist ein Link zur Datei `/usr/lib64/libzfcphbaapi.so`.

Konfigurationsprobleme, die das Fehlen von SAN-Einheiten zur Folge haben, beheben:

Wenn mit dem Serverbefehl **QUERY SAN** nicht alle Einheiten angezeigt werden, kann die mögliche Ursache hierfür ein Konfigurationsproblem mit der HBA-Hardware, der HBA-Treiberversion oder der Betriebssystemversion sein.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um Konfigurationsprobleme zu beheben:

Vorgehensweise

1. Rufen Sie das Support-Portal auf. Überprüfen Sie die Unterstützungsversion für Plattform/HBA-Anbieter/Treiberversion, um sicherzustellen, dass die HBA-Treiberversion und die Betriebssystemversion kompatibel sind und von IBM Spectrum Protect für die SAN-Erkennung unterstützt werden.
2. Verwenden Sie das Dienstprogramm des HBA-Anbieters, um zu überprüfen, ob die Einheit vom HBA angezeigt werden kann. Wenn die Einheit vom HBA nicht angezeigt wird, ist die Einheit möglicherweise nicht angeschlossen. Überprüfen Sie das Fibre-Channel- oder SCSI-Kabel. Wenn die Einheit vom HBA angezeigt wird, überprüfen Sie die HBA-Treiberversion. Diese Treiberversion führt möglicherweise zu Problemen mit der HBA-API.
3. AIX Linux Verwenden Sie das Modul `dsmsanlist`, um Informationen zu Einheiten in einem SAN abzurufen. Das Modul `dsmsanlist` wird bei der Installation des IBM Spectrum Protect-Servers oder des IBM Spectrum Protect-Speicheragenten standardmäßig installiert.

Herstellerunterstützung für eine bestimmte Einheit im SAN überprüfen:

Viele Einheiten oder Kombinationen von Einheiten werden unter Umständen in einem bestimmten Speicherbereichsnetz (SAN) nicht unterstützt. Diese Einschränkungen ergeben sich aus der Möglichkeit eines bestimmten Herstellers, seine Einheiten für die Verwendung des Fibre Channel Protocol zu zertifizieren.

Prüfen Sie für eine bestimmte Einheit mit dem Einheitenhersteller, ob die Einheit in einer SAN-Umgebung unterstützt wird. Die Herstellerunterstützung bezieht sich auf die gesamte Hardware, die dem SAN zugeordnet ist. Dies bedeutet, dass Sie mit den Herstellern der Hostbusadapter, Hubs, Gateways und Switches, die die SAN-Umgebung bilden, sicherstellen müssen, dass diese Einheit unterstützt wird.

Hinweise und Tipps zu Operationen zwischen NDMP-Dateiserver und IBM Spectrum Protect-Server

IBM Spectrum Protect verwendet standardmäßig den NDMP-Steuerungsanschluss 10000 (NDMP = Network Data Management Protocol). Wenn dieser Anschluss von einer anderen Anwendung verwendet wird (z. B. einem zweiten IBM Spectrum Protect-Server), schlagen alle Operationen zwischen dem Dateiserver und dem Server fehl.

Um Konflikte mit anderen Anwendungen zu vermeiden, verwenden Sie die Serveroption `NDMPCONTROLPORT`, um einen anderen Anschluss für Ihren Server anzugeben.

Während der Ausführung von Operationen zwischen dem Dateiserver und dem Server verwendet IBM Spectrum Protect die folgenden Elemente:

- Bis zu zwei zusätzliche TCP/IP-Anschlüsse
- Einen Steuerungsanschluss, der von IBM Spectrum Protect während der Ausführung von Sicherungs- und Zurückschreibungsoperationen intern verwendet wird.
- Einen Datenanschluss während der Ausführung von NDMP-Sicherungsoperationen für einen nativen IBM Spectrum Protect-Speicherpool.

Der Datenanschluss ist ein ephemerer Anschluss, der am Anfang von NDMP-Sicherungsoperationen für einen nativen IBM Spectrum Protect-Speicherpool angefordert wird. Ist ein Anschluss nicht verfügbar, wird eine Fehlernachricht ausgegeben und die Sicherung von NAS-Einheiten in nativen IBM Spectrum Protect-Pools ist nicht möglich. Um Konflikte mit anderen Anwendungen zu vermeiden, können Sie steuern, welcher Anschluss für die Verwendung als Datenanschluss während der Ausführung von NDMP-Sicherungsoperationen angefordert wird, indem Sie die Serveroptionen `NDMPPORTRANGELOW` und `NDMPPORTRANGEHIGH` definieren. Der IBM Spectrum Protect-Server benötigt keinen Datenanschluss, da NAS-Zurückschreibungen aus nativen IBM Spectrum Protect-Pools ausgeführt werden.

Probleme in Bezug auf die Firewall bei der Sicherung und Zurückschreibung zwischen NDMP-Dateiserver und IBM Spectrum Protect-Server

Eine Firewall kann verhindern, dass der NAS-Dateiserver den IBM Spectrum Protect-Server während der Ausführung von NAS-Sicherungsoperationen für einen nativen Speicherpool am angeforderten Datenanschluss ansprechen kann. Wenn Sie den vom IBM Spectrum Protect-Server ausgewählten Datenanschluss ändern müssen, verwenden Sie die Serveroptionen `NDMPPORTRANGELOW` und `NDMPPORTRANGEHIGH`.

Eine Firewall kann verhindern, dass der IBM Spectrum Protect-Server den NAS-Dateiserver während der Ausführung von NAS-Zurückschreibungsoperationen aus einem nativen Speicherpool an dem konfigurierten Datenanschluss ansprechen kann. Wenn eine Firewall den Zugriff von IBM Spectrum Protect auf den NAS-Dateiserver verhindert, schlägt die abgehende Verbindung von IBM Spectrum Protect fehl.

SCSI-Einheitenfehler beheben

Bandlaufwerke und -archive können Informationen zu dem festgestellten Fehler an IBM Spectrum Protect zurückmelden. Diese Informationen werden in einer oder in mehreren Nachrichten zurückgemeldet.

Wenn die Nachricht ANR8300, ANR8301, ANR8302, ANR8303, ANR8943 oder ANR98944 ausgegeben wird, können die Daten, die von IBM Spectrum Protect zu diesen Einheiten zurückgemeldet werden, bei der Bestimmung der Schritte helfen, die zur Behebung des Problems ausgeführt werden müssen. Wenn der Server Einheitendaten mithilfe dieser Nachrichten zurückmeldet, wird der Fehler normalerweise durch die Einheit, durch die Verbindung zur Einheit oder durch ein anderes verwandtes Problem außerhalb von IBM Spectrum Protect verursacht.

Ziehen Sie unter Verwendung der Informationen, die in der IBM Spectrum Protect-Nachricht ANR8300, ANR8301, ANR8302, ANR8303, ANR8943 oder ANR8944 zurückgemeldet werden, die Produktinformation mit den IBM Spectrum Protect-Nachrichten unter Nachrichten, Rückkehrcodes und Fehlercodes zu Rate. In diesem Anhang sind Informationen zu Standardfehlern dokumentiert, die von jeder SCSI-Einheit zurückgemeldet werden können. Sie können diese Informationen auch mit der Dokumentation verwenden, die vom Hersteller der Hardware bereitgestellt wird, um die Ursache und Lösung des Problems zu bestimmen.

Fehler bei Datenträgern mit sequenziellem Zugriff (Band) durch Nachricht ANR0542W oder ANR8778W beheben

Probleme, die mit sequenziellen Datenträgern auftreten, können durch die Fehlernachrichten ANR0542W und ANR8778W sichtbar gemacht werden.

ANR0542W Abrufen oder Zurückschreiben für Sitzung *Sitzungsnummer* für Knoten *Knotenname* fehlgeschlagen - kein Zugriff auf Speicherdatenträger möglich.

Die Fehlernachricht ANR0542W bezieht sich oft auf ein Problem mit dem Laufwerk oder der Verbindung zum Laufwerk, das zum Lesen dieses Banddatenträgers ausgewählt wurde.

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob IBM Spectrum Protect auf diesen Datenträger zugreifen kann:

- Geben Sie den Befehl `QUERY LIBVOL` *`Kassettenarchivname Datenträgername`* aus.
- Geben Sie für ein 349X-Kassettenarchiv den Befehl `mtlib -l /dev/lmcp0 -qV` *`Datenträgername`* aus. Die Einheit ist normalerweise `/dev/lmcp0`. Handelt es sich jedoch um eine andere Einheit, setzen Sie die korrekte LMCP-Einheit ein (LMCP = Library Manager Control Point).

Mit den folgenden Schritten kann dieses Problem möglicherweise behoben werden:

1. Wenn 'mtlib' diesen Datenträger nicht zurückmeldet, scheint sich dieser Datenträger außerhalb des Archivs zu befinden. Stellen Sie in diesem Fall den Datenträger wieder in das Archiv.
2. Wird der Datenträger von `QUERY LIBVOL` nicht zurückgemeldet, ist dem Server dieser Datenträger im Archiv nicht bekannt. Geben Sie den Befehl **`CHECKIN LIBVOL`** aus, um den Archivbestand auf dem Server mit den Datenträgern zu synchronisieren, die sich tatsächlich im Bandarchiv befinden.
3. Wenn beide Befehle diesen Datenträger erfolgreich zurückmelden, ist die Ursache wahrscheinlich ein permanenter oder periodisch auftretender Hardwarefehler. Es kann ein Fehler bei dem Laufwerk selbst oder ein Fehler bei der Verbindung zum Laufwerk vorliegen. Überprüfen Sie in beiden Fällen die Systemfehlerprotokolle und wenden Sie sich an den Hersteller der Hardware, um das Problem zu beheben.

ANR8778W Arbeitsdatenträger in Status 'Private' geändert, um erneuten Zugriff zu verhindern.

Überprüfen Sie die Nachrichten im Aktivitätenprotokoll, um die Ursache des Problems in Bezug auf diesen Arbeitsdatenträger zu bestimmen. Überprüfen Sie auch die Systemfehlerprotokolle und Einheitenfehlerprotokolle auf einen Hinweis, dass ein Problem mit dem Laufwerk aufgetreten ist, das zum Schreiben auf diesen Arbeitsdatenträger verwendet wurde.

Wenn dieser Fehler durch ein Laufwerk, das eine Reinigung erfordert hat, oder durch ein anderes hardwarespezifisches Problem, das behoben wurde, aufgetreten ist, können alle Datenträger, die aufgrund dieses Fehlers in den Status 'Private' versetzt wurden, mit dem Befehl `AUDIT LIBRARY` *`Kassettenarchivname`* wieder in den Arbeitsdatenträgerstatus versetzt werden.

Anhang A. Aufrufstackinformationen aus einer Kerndatei abrufen

Sie können die hier bereitgestellte gt-Beispielscript-Shell verwenden, um den Aufrufstack für jeden aktiven Thread aus einer Kerndatei abzurufen.

Die Eingabeparameter sind der Pfad/Name der ausführbaren Datei (Standardwert ./dsmserv) und der Pfad/Name der Kerndatei (Standardwert ./dsmcore). Die Ausgabedatei ist `dsm_gdb.info`.

Einschränkung: Dateien mit dem Namen `dsm_gdb.cmd` und `dsm_gdb.info` werden bei der Ausführung dieses Scripts überschrieben.

```
#!/bin/ksh
#
# If you see the following error:
# ./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
```

Anhang B. Dienstprogramm 'tsmdiag' ausführen

Sie können Probleme bei einem IBM Spectrum Protect-Server diagnostizieren, indem Sie das Dienstprogramm 'tsmdiag' auf dem System ausführen, auf dem der IBM Spectrum Protect-Server installiert ist. Nach der Erfassung der Diagnosedaten können Sie die Informationen zum IBM Software Support senden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das Dienstprogramm 'tsmdiag' auszuführen:

1. AIX Linux Ändern Sie die Berechtigungen für das Verzeichnis `tsmdiag` durch Ausgabe des folgenden Befehls:

   ```
   chmod -R 757 /opt/tivoli/tsm/server/bin/tsmdiag
   ```

2. Geben Sie den Befehl **tsmdiag** im folgenden Verzeichnis aus:

   - AIX Linux Sie müssen unter Verwendung einer Benutzer-ID für die DB2-Instanz den Befehl **tsmdiag** im Verzeichnis `/opt/tivoli/tsm/server/bin/tsmdiag` ausgeben.
   - Windows Sie müssen unter Verwendung einer Benutzer-ID mit Administratorberechtigung den Befehl **tsmdiag** im Verzeichnis `\server\tsmdiag` ausführen.

   Der folgende Befehl beispielsweise erfasst eine Standardgruppe von Diagnoseinformationsdateien von einem IBM Spectrum Protect-Server auf einem lokalen Host. Dieser Befehl wird von einem Administrator mit dem Namen 'admin' und dem Administratorkennwort 'admin01' auf einem IBM Spectrum Protect-Server ausgeführt. Dieser Server ist am TCP/IP-Port 1501 auf einem lokalen Host aktiv.

   ```
   tsmdiag -id admin -pa admin01 -tcpport 1501
   ```

3. Rufen Sie die Ergebnisdatei aus dem folgenden Verzeichnis ab:

   - AIX Linux `/opt/tivoli/tsm/server/bin/tsmdiag/results/tsmdiag_results<Jahr>-<Monat>-<Tag>-<Stunde>-<Minute>-<Sekunde>.tar`
   - Windows `C:\Programme\tivoli\tsm\server\tsmdiag\results\tsmdiag_results<Jahr>-<Monat>-<Tag>-<Stunde>-<Minute>-<Sekunde>.zip`

4. Übergeben Sie die Ergebnisdatei mit dem Problembericht an den IBM Software Support.

tsmdiag-Beispielbefehle

Der folgende Befehl stellt eine Verbindung zu einem IBM Spectrum Protect-Server mit Namen MYSERVER am TCP/IP-Port 1501 her. Wenn ein DB2-Administrator mit Namen 'admin' den folgenden Befehl ausführt, wird eine Standardgruppe von Diagnoseinformationsdateien erfasst. Außerdem werden Diagnoseinformationen zur Leistung des Servers MYSERVER erfasst.

```
tsmdiag -id admin -pa admin01 -tcpport 1501 -servername MYSERVER -performance
```

Der folgende Befehl stellt eine Verbindung zu einem IBM Spectrum Protect-Server am TCP/IP-Standardport 1500 her. Wenn ein Administrator mit Namen 'admin' den folgenden Befehl ausführt, erfasst der Befehl eine Standardgruppe von Diagnoseinformationsdateien. Dieser Befehl stellt außerdem Ergebnisse aus den **SHOW**-

Befehlen des IBM Spectrum Protect-Servers sowie eine Reihe von Diagnoseinformationen zum Status des IBM Spectrum Protect-Servers bereit.

```
tsmdiag -id admin -pa admin01 -hang
```

Optionen für das Dienstprogramm 'tsmdiag'

Das Dienstprogramm 'tsmdiag' unterstützt das Diagnostizieren von Problemen bei einer IBM Spectrum Protect-Serverkomponente. Bei der Ausführung des Dienstprogramms können Sie Optionen angeben, die den Typ der Diagnoseinformationen festlegen, die bereitgestellt werden.

Für den Befehl **tsmdiag** können Sie die folgenden Optionen angeben:

id *Administratorname*
Die Administrator- oder Rootbenutzer-ID des Servers, auf dem der Befehl **tsmdiag** ausgeführt werden soll. Diese Option ist obligatorisch.

-pa *Administratorkennwort*
Das Kennwort für die Administrator- oder Rootbenutzer-ID. Diese Option ist obligatorisch.

-tcpserveraddress *IP-Adresse*
Gibt den TCP/IP-Namen oder die Adresse des Servers an, auf dem der Befehl **tsmdiag** ausgeführt werden soll. Diese Option ist optional. Der Standardwert ist `localhost`.

-tcpport *Portnummer*
Gibt den TCP/IP-Port des Servers an, auf dem der Befehl **tsmdiag** ausgeführt werden soll. Diese Option ist optional. Der Standardwert ist `1500`.

AIX Linux **-servername**
Der Name des Servers, auf dem der Befehl **tsmdiag** ausgeführt werden soll. Diese Option ist optional. Der Standardwert ist `SERVER1`.

-crash Gibt an, ob gemeldet werden soll, wenn der Server ausfällt. Diese Option ist optional. Der Standardwert ist `off`.

-dbcorrupt
Gibt an, ob gemeldet werden soll, wenn eine Beschädigung der Datenbank vorliegt. Diese Option ist optional. Der Standardwert ist `off`.

-dbgrowth
Gibt an, ob gemeldet werden soll, wenn Datenbanken auf dem Server übermäßig an Größe zunehmen. Diese Option führt die Scripts `serverReorgInfo.pl` und `tsmdiag_dedup_stats.pl` aus, die zusätzliche Diagnoseinformationen erstellen. Die Ausführung des Scripts `serverReorgInfo.pl` dauert über eine Stunde. Diese Option ist optional. Der Standardwert ist `off`.

-hang Gibt an, ob gemeldet werden soll, wenn der Server blockiert ist. Diese Option ist optional. Der Standardwert ist `off`.

-performance
Gibt an, ob gemeldet werden soll, wenn Leistungsprobleme beim Server vorliegen. Diese Option führt das Script `tsmdiag_sysmonv6.pl` aus, das zusätzliche Diagnoseinformationen erstellt. Die Ausführung des Scripts `tsmdiag_sysmonv6.pl` kann eineinhalb Stunden dauern. Diese Option ist optional. Der Standardwert ist `off`.

-v Gibt an, dass die Berichtsausgabe im ausführlichen Format erstellt wird. Diese Option ist optional. Der Standardwert ist `off`.

-? Gibt die Syntaxinformationen für das Dienstprogramm 'tsmdiag' an. Falls Sie den Befehl `tsmdiag ?` absetzen, wird eine Liste der obigen Optionen angezeigt.

Anhang C. Rückkehrcodes für IBM Global Security Kit

Der Server und Client verwenden das IBM Global Security Kit (GSKit) für die SSL-Verarbeitung (SSL - Secure Sockets Layer) zwischen dem Server und dem Client für Sichern/Archivieren. Einige Nachrichten, die für die SSL-Verarbeitung ausgegeben werden, enthalten GSKit-Rückkehrcodes.

GSKit wird während der IBM Spectrum Protect-Installation automatisch installiert oder aktualisiert und stellt die folgenden Bibliotheken bereit:

- GSKit SSL
- GSKit Key Management API
- IBM Crypto for C (ICC)

Mit dem Dienstprogramm 'tsmdiag' wird die auf Ihrem System installierte GSKit-Version zurückgemeldet. Sie können auch eine der folgenden Methoden verwenden:

- Geben Sie für Windows die folgenden Befehle aus:

  ```
  regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\"
  notepad gskitinfo.txt
  ```

  Vorsicht:
  Sie können das Systemregistry beschädigen, wenn Sie 'regedit' nicht ordnungsgemäß verwenden.
- Geben Sie für den AIX-Server (64-Bit) den folgenden Befehl in der Befehlszeile aus: `gsk8ver_64`

Tabelle 17 enthält die GSKit SSL-Rückkehrcodes.

Der Server verwendet die GSKit Key Management API, um die Schlüsselmanagementdatenbank und die privaten und öffentlichen Schlüssel des Servers automatisch zu erstellen. Einige Nachrichten, die für diese Verarbeitung ausgegeben werden, können GSKit Key Management-Rückkehrcodes einschließen. Tabelle 18 auf Seite 222 enthält die Key Management-Rückkehrcodes.

Tabelle 17. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000000	0	`GSK_OK`	Die Task wurde erfolgreich ausgeführt. Wird von jedem Funktionsaufruf ausgegeben, der erfolgreich ausgeführt wird.
0x00000001	1	`GSK_INVALID_HANDLE`	Die Umgebungskennung oder SSL-Kennung ist nicht gültig. Die angegebene Kennung war nicht das Ergebnis eines erfolgreichen Funktionsaufrufs `open()`.
0x00000002	2	`GSK_API_NOT_AVAILABLE`	Die DLL-Datei wurde entladen und ist nicht verfügbar (tritt nur auf Microsoft Windows-Systemen auf).
0x00000003	3	`GSK_INTERNAL_ERROR`	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.

Tabelle 17. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000004	4	GSK_INSUFFICIENT_STORAGE	Für die Ausführung der Operation ist nicht genügend Speicher verfügbar.
0x00000005	5	GSK_INVALID_STATE	Die Kennung hat keinen gültigen Status für die Operation, z. B. bei zweimaliger Ausführung einer Operation `init()` für eine Kennung.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	Der angegebene Schlüsselkennsatz wurde nicht in der Schlüsseldatei gefunden.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	Zertifikat nicht vom Partner empfangen.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Fehler bei der Zertifikatsvalidierung.
0x00000009	9	GSK_ERROR_CRYPTO	Fehler bei der Verarbeitung der Verschlüsselung.
0x0000000a	10	GSK_ERROR_ASN	Fehler bei der Validierung von ASN-Feldern im Zertifikat.
0x0000000b	11	GSK_ERROR_LDAP	Fehler beim Herstellen der Verbindung zur Benutzerregistry.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x0000000d	13	GSK_INVALID_PARAMETER	Ungültiger Parameter.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Ungültiger Parameter. Melden Sie diesen Fehler dem IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	E/A-Fehler beim Lesen der Schlüsseldatei.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	Die Schlüsseldatei hat kein gültiges internes Format. Erstellen Sie die Schlüsseldatei erneut.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	Die Schlüsseldatei hat zwei Einträge mit demselben Schlüssel.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	Die Schlüsseldatei hat zwei Einträge mit demselben Kennsatz.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	Das Kennwort für die Schlüsseldatei wird als Integritätsprüfung verwendet. Entweder ist die Schlüsseldatei beschädigt oder die Kennwort-ID ist falsch.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	Der Standardschlüssel in der Schlüsseldatei hat ein abgelaufenes Zertifikat.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Beim Laden einer der GSK DLL-Dateien ist ein Fehler aufgetreten. Überprüfen Sie, ob GSK korrekt installiert wurde.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Gibt an, dass eine Verbindung in einer GSK-Umgebung hergestellt werden soll, nachdem `GSK_ENVIRONMENT_CLOSE_OPTIONS` auf `GSK_DELAYED_ ENVIRONMENT_CLOSE` gesetzt und die Funktion `gsk_environment_close()` aufgerufen wurde.

Tabelle 17. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	Weder das Kennwort noch der Name der Stashdatei wurde angegeben. Die Schlüsseldatei wurde nicht initialisiert.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Die Schlüsseldatei kann nicht geöffnet werden. Entweder wurde der Pfad nicht korrekt angegeben oder die Dateiberechtigungen erlauben nicht das Öffnen der Datei.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Temporäres Schlüsselpaar kann nicht generiert werden. Melden Sie diesen Fehler dem IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Das angegebene Benutzernamenobjekt wurde nicht gefunden.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Ein Kennwort, das für eine LDAP-Abfrage (LDAP = Lightweight Directory Access Protocol) verwendet wird, ist nicht korrekt.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Ein Index in der Übernahmeliste der LDAP-Server war nicht korrekt.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Diese Installation von GSKit unterstützt nicht die FIPS-Betriebsart.
0x0000012d	301	GSK_CLOSE_FAILED	Gibt an, dass die Anforderung zum Schließen der GSK-Umgebung nicht korrekt ausgeführt wurde. Die Ursache ist wahrscheinlich ein Befehl `gsk_secure_socket*()`, der nach einem Aufruf `gsk_close_environment()` ausgeführt werden sollte.
0x00000191	401	GSK_ERROR_BAD_DATE	Das Systemdatum wurde nicht auf einen gültigen Wert gesetzt.
0x00000192	402	GSK_ERROR_NO_CIPHERS	SSLv2 und SSLv3 sind nicht aktiviert.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	Das erforderliche Zertifikat wurde nicht vom Partner empfangen.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	Das empfangene Zertifikat war nicht korrekt formatiert.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	Der empfangene Zertifikatstyp wurde nicht unterstützt.
0x00000196	406	GSK_ERROR_IO	Ein E/A-Fehler ist bei einer Datenlese- oder -schreiboperation aufgetreten.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	Der angegebene Schlüsseldateikennsatz wurde nicht gefunden.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	Das angegebene Kennwort für die Schlüsseldatei ist falsch. Die Schlüsseldatei kann nicht verwendet werden. Die Schlüsseldatei kann auch beschädigt sein.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	In einer eingeschränkten Verschlüsselungsumgebung wird die Schlüsselgröße nicht unterstützt.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Eine falsch formatierte SSL-Nachricht wurde vom Partner empfangen.

Tabelle 17. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x0000019b	411	GSK_ERROR_BAD_MAC	Der Nachrichtenauthentifizierungscode wurde nicht erfolgreich überprüft.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Nicht unterstütztes SSL-Protokoll oder nicht unterstützter Zertifikatstyp.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	Das empfangene Zertifikat enthielt eine falsche Signatur.
0x0000019e	414	GSK_ERROR_BAD_CERT	Falsch formatiertes Zertifikat vom Partner empfangen.
0x0000019f	415	GSK_ERROR_BAD_PEER	Kein gültiges SSL-Protokoll vom Partner empfangen.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	Das selbst signierte Zertifikat ist nicht gültig.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	`read()` ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	`write()` ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	Der Partner hat das Socket geschlossen, bevor das Protokoll beendet war.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	Die angegebene V2-Verschlüsselung ist nicht gültig.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	Die angegebene V3-Verschlüsselung ist nicht gültig.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	Die Kennung kann nicht erstellt werden. Melden Sie diesen Fehler dem IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Initialisierung ist fehlgeschlagen. Melden Sie diesen internen Fehler dem Service.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Bei der Überprüfung eines Zertifikats kann nicht auf die angegebene Benutzerregistry zugegriffen werden.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	Der angegebene Schlüssel enthielt keinen privaten Schlüssel.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Der Versuch, die angegebene gemeinsam genutzte PKCS11-Bibliothek zu laden, ist fehlgeschlagen.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	Der PKCS #11-Treiber konnte das vom aufrufenden Programm angegebene Token nicht finden.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	Ein PKCS #11-Token ist in dem Bereich nicht vorhanden.

Tabelle 17. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	Das Kennwort/die PIN für den Zugriff auf das PKCS #11-Token ist nicht gültig.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	Der empfangene SSL-Header war kein korrekt formatierter SSLv2-Header.
0x000001b2	434	GSK_CSP_OPEN_ERROR	Der hardwarebasierte Verschlüsselungsserviceanbieter (Cryptographic Service Provider = CSP) kann nicht geöffnet werden. Entweder ist der CSP-Name nicht korrekt angegeben oder ein Versuch, auf den angegebenen CSP-Zertifikatsspeicher zuzugreifen, ist fehlgeschlagen.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Konflikt bei der Attributeinstellung zwischen PKCS11, der CMS-Schlüsseldatenbank und der Microsoft Krypto-API.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	Die angeforderte Funktion wird auf der Plattform, die von der Anwendung ausgeführt wird, nicht unterstützt. Die Microsoft Krypto-API wird beispielsweise nur auf der Plattform Windows 2000 unterstützt.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Ein falscher Wert wird von der Callback-Funktion zum Zurücksetzen des Sitzungstyps zurückgegeben. Nur GSKit `gsk_sever_session`, `gsk_sever_session_with_cl_auth` oder `gsk_sever_session_with_cl_auth_crit` ist zulässig.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	Die Puffergröße ist negativ oder Null.
0x000001f6	502	GSK_WOULD_BLOCK	Wird mit nicht geblockter Ein-/Ausgabe verwendet. Siehe den Abschnitt zur nicht geblockten Ein-/Ausgabe.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 ist für `reset_cipher()` erforderlich, und die Verbindung verwendet SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Es wurde keine gültige ID für den Funktionsaufruf `gsk_secure_soc_misc()` angegeben.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	Der Funktionsaufruf hat keine gültige ID. Dieses Problem kann auch durch die Angabe einer Umgebungskennung verursacht werden, wenn stattdessen eine Kennung für eine SSL-Verbindung verwendet werden müsste.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	Das Attribut hat eine negative Länge, die nicht gültig ist.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	Der Aufzählungswert ist für den angegebenen Aufzählungstyp nicht gültig.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Eine Parameterliste, die zum Ersetzen der SID-Cacheroutinen nicht gültig ist.

Tabelle 17. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Beim Definieren eines numerischen Attributs ist der angegebene Wert für das spezielle Attribut, das definiert wird, nicht gültig.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Für die zusätzliche Zertifikatsvalidierung wurden sich widersprechende Parameter definiert.
0x000002c3	707	GSK_AES_UNSUPPORTED	Der AES-Verschlüsselungsalgorithmus wird nicht unterstützt.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	Die PEERID hat nicht die korrekte Länge.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	Der betreffende Chiffrierwert ist nicht zulässig, wenn die FIPS-Betriebsart auf OFF gesetzt ist.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	In der FIPS-Betriebsart sind keine genehmigten FIPS-Chiffrierwerte ausgewählt.
0x00000641	1601	GSK_TRACE_STARTED	Der Trace wurde erfolgreich gestartet.
0x00000642	1602	GSK_TRACE_STOPPED	Der Trace wurde erfolgreich gestoppt.
0x00000643	1603	GSK_TRACE_NOT_STARTED	Es wurde zuvor keine Tracedatei gestartet. Daher kann sie nicht gestoppt werden.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	Die Tracedatei wurde bereits gestartet. Daher kann sie nicht erneut gestartet werden.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	Die Tracedatei kann nicht geöffnet werden. Der erste Parameter von `gsk_start_trace()` muss ein gültiger vollständiger Pfaddateiname sein.

Tabelle 18. IBM Global Security Kit Key Management-Rückkehrcodes

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000000	0	GSK_OK	Die Task wurde erfolgreich ausgeführt. Diese Nachricht wird von jedem Funktionsaufruf ausgegeben, der erfolgreich ausgeführt wird.
0x00000001	1	GSK_INVALID_HANDLE	Die Umgebungskennung oder SSL-Kennung ist nicht gültig. Die angegebene Kennung war nicht das Ergebnis eines erfolgreichen Funktionsaufrufs open().
0x00000002	2	GSK_API_NOT_AVAILABLE	Die DLL-Datei (DLL = Dynamic Link Library) wurde entladen und ist nicht verfügbar (tritt nur auf Microsoft Windows-Systemen auf).
0x00000003	3	GSK_INTERNAL_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	Für die Ausführung der Operation ist nicht genügend Speicher verfügbar.

Tabelle 18. IBM Global Security Kit Key Management-Rückkehrcodes (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000005	5	GSK_INVALID_STATE	Die Kennung hat einen falschen Status für die Operation, z. B. bei zweimaliger Ausführung einer Operation init() für eine Kennung.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	Der angegebene Schlüsselkennsatz wurde nicht in der Schlüsseldatei gefunden.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	Zertifikat nicht vom Partner empfangen.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Fehler bei der Zertifikatsvalidierung.
0x00000009	9	GSK_ERROR_CRYPTO	Fehler bei der Verarbeitung der Verschlüsselung.
0x0000000a	10	GSK_ERROR_ASN	Fehler bei der Validierung von ASN-Feldern im Zertifikat.
0x0000000b	11	GSK_ERROR_LDAP	Fehler beim Herstellen der Verbindung zur Benutzerregistry.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	E/A-Fehler beim Lesen der Schlüsseldatei.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	Die Schlüsseldatei hat ein internes Format, das nicht gültig ist. Die Schlüsseldatei erneut erstellen.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	Die Schlüsseldatei hat zwei Einträge mit demselben Schlüssel.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	Die Schlüsseldatei hat zwei Einträge mit demselben Kennsatz.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_ PASSWORD	Das Kennwort für die Schlüsseldatei wird als Integritätsprüfung verwendet. Entweder ist die Schlüsseldatei beschädigt oder die Kennwort-ID ist falsch.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	Der Standardschlüssel in der Schlüsseldatei hat ein abgelaufenes Zertifikat.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Beim Laden einer der GSK DLL-Dateien ist ein Fehler aufgetreten. Überprüfen Sie, ob GSK korrekt installiert wurde.

Tabelle 18. IBM Global Security Kit Key Management-Rückkehrcodes (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Diese Nachricht gibt an, dass eine Verbindung in einer GSK-Umgebung hergestellt werden soll, nachdem GSK_ENVIRONMENT_CLOSE_OPTIONS auf GSK_DELAYED_ ENVIRONMENT_CLOSE gesetzt und die Funktion gsk_environment_close() aufgerufen wurde.
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	Es wurde weder das Kennwort noch der Stashdateiname angegeben, daher konnte die Schlüsseldatei nicht initialisiert werden.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Die Schlüsseldatei kann nicht geöffnet werden. Entweder wurde der Pfad nicht korrekt angegeben oder die Dateiberechtigungen erlauben nicht das Öffnen der Datei.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Temporäres Schlüsselpaar kann nicht generiert werden. Melden Sie diesen Fehler dem IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Das angegebene Benutzernamenobjekt wurde nicht gefunden.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_ CREDENTIALS	Ein Kennwort, das für eine LDAP-Abfrage verwendet wird, ist nicht korrekt.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Ein Index in der Übernahmeliste der LDAP-Server war nicht korrekt.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Diese Installation von GSKit unterstützt nicht die FIPS-Betriebsart.
0x0000012d	301	GSK_CLOSE_FAILED	Gibt an, dass die Anforderung zum Schließen der GSK-Umgebung nicht korrekt ausgeführt wurde. Die Ursache ist wahrscheinlich ein Befehl gsk_secure_socket*(), der nach einem Aufruf gsk_close_environment() ausgeführt werden sollte.
0x00000191	401	GSK_ERROR_BAD_DATE	Das Systemdatum wurde auf einen Wert gesetzt, der nicht gültig ist.
0x00000192	402	GSK_ERROR_NO_CIPHERS	SSLv2 und SSLv3 sind nicht aktiviert.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	Das erforderliche Zertifikat wurde nicht vom Partner empfangen.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	Das empfangene Zertifikat war nicht korrekt formatiert.

Tabelle 18. IBM Global Security Kit Key Management-Rückkehrcodes (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000195	405	GSK_ERROR_UNSUPPORTED_ CERTIFICATE_TYPE	Der empfangene Zertifikatstyp wurde nicht unterstützt.
0x00000196	406	GSK_ERROR_IO	Ein E/A-Fehler ist bei einer Datenlese- oder -schreiboperation aufgetreten.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	Der angegebene Schlüsseldateikennsatz wurde nicht gefunden.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	Das angegebene Kennwort für die Schlüsseldatei ist falsch. Die Schlüsseldatei kann nicht verwendet werden. Die Schlüsseldatei könnte auch beschädigt sein.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_ FOR_EXPORT	In einer eingeschränkten Verschlüsselungsumgebung wird die Schlüsselgröße nicht unterstützt.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Eine falsch formatierte SSL-Nachricht wurde vom Partner empfangen.
0x0000019b	411	GSK_ERROR_BAD_MAC	Der Nachrichtenauthentifizierungscode wurde nicht erfolgreich verifiziert.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Nicht unterstütztes SSL-Protokoll oder nicht unterstützter Zertifikatstyp.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	Das empfangene Zertifikat enthielt eine falsche Signatur.
0x0000019e	414	GSK_ERROR_BAD_CERT	Falsch formatiertes Zertifikat vom Partner empfangen.
0x0000019f	415	GSK_ERROR_BAD_PEER	Ein ungültiges SSL-Protokoll wurde vom Partner empfangen.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	Das selbst signierte Zertifikat ist nicht gültig.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	read() ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	write() ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	Der Partner hat das Socket geschlossen, bevor das Protokoll beendet war.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	Die angegebene V2-Verschlüsselung ist nicht gültig.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	Die angegebene V3-Verschlüsselung ist nicht gültig.

Tabelle 18. IBM Global Security Kit Key Management-Rückkehrcodes (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_ COMBINATION	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_ FAILED	Die Kennung wurde nicht erstellt. Melden Sie diesen Fehler dem IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Initialisierung ist fehlgeschlagen. Melden Sie diesen internen Fehler dem Service.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Bei der Überprüfung eines Zertifikats kann nicht auf die angegebene Benutzerregistry zugegriffen werden.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	Der angegebene Schlüssel enthielt keinen privaten Schlüssel.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_ NOTLOADED	Der Versuch, die angegebene gemeinsam genutzte PKCS11-Bibliothek zu laden, ist fehlgeschlagen.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_ LABELMISMATH	Der PKCS #11-Treiber konnte das vom aufrufenden Programm angegebene Token nicht finden.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_ NOTPRESENT	Ein PKCS #11-Token ist in dem Bereich nicht vorhanden.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_ BADPASSWORD	Das Kennwort/die PIN für den Zugriff auf das PKCS #11-Token ist falsch.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	Der empfangene SSL-Header war kein korrekt formatierter SSLv2-Header.
0x000001b2	434	GSK_CSP_OPEN_ERROR	Der hardwarebasierte Verschlüsselungsserviceanbieter (Cryptographic Service Provider = CSP) konnte nicht geöffnet werden. Entweder ist der CSP-Name nicht korrekt angegeben oder ein Versuch, auf den angegebenen CSP-Zertifikatsspeicher zuzugreifen, ist fehlgeschlagen.
0x000001b3	435	GSK_CSP_OPEN_ERROR	Einige sich widersprechende Attribute für die SSL-Operation wurden definiert.
0x000001b4	436	GSK_CSP_OPEN_ERROR	Die Microsoft Crypto API wird nur unter Microsoft Windows 2000 mit Service-Pack 2 unterstützt.
0x000001b5	437	GSK_CSP_OPEN_ERROR	System wird im IPv6-Modus ausgeführt, ohne dass eine PEERID definiert ist.

Tabelle 18. IBM Global Security Kit Key Management-Rückkehrcodes (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	Die Puffergröße ist negativ oder Null.
0x000001f6	502	GSK_WOULD_BLOCK	Wird mit nicht geblockter Ein-/Ausgabe verwendet. Siehe den Abschnitt zur nicht geblockten Ein-/Ausgabe.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 ist für reset_cipher() erforderlich, und die Verbindung verwendet SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Eine ungültige ID wurde für den Funktionsaufruf gsk_secure_soc_misc() angegeben.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	Der Funktionsaufruf hat eine ID, die nicht gültig ist. Dieses Problem kann auch durch die Angabe einer Umgebungskennung verursacht werden, wenn stattdessen eine Kennung für eine SSL-Verbindung verwendet werden müsste.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	Das Attribut hat eine negative Länge, die nicht gültig ist.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ ENUMERATION	Der Aufzählungswert ist für den angegebenen Aufzählungstyp nicht gültig.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Eine Parameterliste, die zum Ersetzen der SID-Cacheroutinen nicht gültig ist.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_ NUMERIC_VALUE	Beim Definieren eines numerischen Attributs ist der angegebene Wert für das spezielle Attribut, das definiert wird, nicht gültig.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_ SETTING	Für die zusätzliche Zertifikatsvalidierung wurden sich widersprechende Parameter definiert.
0x000002c3	707	GSK_AES_UNSUPPORTED	Der AES-Verschlüsselungsalgorithmus wird nicht unterstützt.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	Die PEERID hat nicht die korrekte Länge.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	Der betreffende Chiffrierwert ist nicht zulässig, wenn die FIPS-Betriebsart auf OFF gesetzt ist.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	In der FIPS-Betriebsart sind keine genehmigten FIPS-Chiffrierwerte ausgewählt.
0x00000641	1601	GSK_TRACE_STARTED	Der Trace wurde erfolgreich gestartet.

Tabelle 18. IBM Global Security Kit Key Management-Rückkehrcodes (Forts.)

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000642	1602	GSK_TRACE_STOPPED	Der Trace wurde erfolgreich gestoppt.
0x00000643	1603	GSK_TRACE_NOT_STARTED	Es wurde zuvor keine Tracedatei gestartet. Daher kann sie nicht gestoppt werden.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	Die Tracedatei wurde bereits gestartet. Daher kann sie nicht erneut gestartet werden.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	Die Tracedatei kann nicht geöffnet werden. Der erste Parameter von gsk_start_trace() muss ein gültiger vollständiger Pfaddateiname sein.

Anhang D. Funktionen zur behindertengerechten Bedienung für die IBM Spectrum Protect-Produktfamilie

Funktionen zur behindertengerechten Bedienung helfen Benutzern mit Behinderungen, wie eingeschränkter Beweglichkeit oder Sehfähigkeit, damit sie informationstechnologische Inhalte erfolgreich verwenden können.

Übersicht

Die IBM Spectrum Protect-Produktfamilie umfasst die folgenden bedeutenden Funktionen zur behindertengerechten Bedienung:

- Bedienung ausschließlich über die Tastatur
- Operationen, die ein Sprachausgabeprogramm verwenden

Die IBM Spectrum Protect-Produktfamilie verwendet den neuesten W3C-Standard WAI-ARIA 1.0(www.w3.org/TR/wai-aria/), um die Einhaltung von US Section 508(www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) und der Web Content Accessibility Guidelines (WCAG) 2.0(www.w3.org/TR/WCAG20/) sicherzustellen. Um die Funktionen zur behindertengerechten Bedienung zu nutzen, verwenden Sie das neueste Release Ihres Sprachausgabeprogramms in Verbindung mit dem neuesten Web-Browser, der von diesem Produkt unterstützt wird.

Die Produktdokumentation im IBM Knowledge Center ist für die behindertengerechte Bedienung aktiviert. Eine Beschreibung der Funktionen zur behindertengerechten Bedienung im IBM Knowledge Center finden Sie im Abschnitt 'Accessibility' der IBM Knowledge Center-Hilfe (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navigation mithilfe der Tastatur

Dieses Produkt verwendet Standardnavigationstasten.

Schnittstelleninformationen

In den Benutzerschnittstellen gibt es keine Inhalte, die 2 - 55 Mal in der Sekunde blinken.

Die Webbenutzerschnittstellen basieren auf Cascading Style Sheets, um Inhalte ordnungsgemäß wiederzugeben und um positive Erfahrungen zu ermöglichen. Die Anwendung bietet eine funktional entsprechende Möglichkeit für Benutzer mit eingeschränktem Sehvermögen, um die Systemanzeigeeinstellungen des Benutzers einschließlich des Modus für kontraststarke Anzeige zu verwenden. Sie können die Schriftgröße über die Einstellungen für die Einheit oder für den Web-Browser steuern.

Die Webbenutzerschnittstellen beinhalten WAI-ARIA-Navigationsmarkierungen, mit deren Hilfe Sie schnell zu Funktionsbereichen in der Anwendung navigieren können.

Software anderer Anbieter

Die IBM Spectrum Protect-Produktfamilie enthält bestimmte Software anderer Anbieter, die nicht der IBM Lizenzvereinbarung unterliegt. IBM gibt keine Erklärung zu den Funktionen zur behindertengerechten Bedienung dieser Produkte ab. Wenden Sie sich an den Softwareanbieter, um Informationen zur behindertengerechten Bedienung der Produkte zu erhalten.

Zugehörige Informationen zur behindertengerechten Bedienung

Neben dem standardmäßigen IBM Help-Desk und den Support-Websites bietet IBM einen TTY-Telefonservice für gehörlose oder hörgeschädigte Kunden für den Zugriff auf Vertriebs- und Support-Services:

TTY-Service
800-IBM-3383 (800-426-3383)
(innerhalb von Nordamerika)

Weitere Informationen zum Engagement von IBM im Bereich der behindertengerechten Bedienung finden Sie in IBM Accessibility (www.ibm.com/able).

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. IBM stellt dieses Material möglicherweise auch in anderen Sprachen zur Verfügung. Für den Zugriff auf das Material in einer anderen Sprache kann eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich sein.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die in diesem Dokument enthaltenen Leistungsdaten wurden von bestimmten Betriebsbedingungen abgeleitet. Die tatsächlichen Ergebnisse können davon abweichen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten: © (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Website "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Adobe ist eine eingetragene Marke der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Linear Tape-Open, LTO und Ultrium sind Marken von HP, der IBM Corporation und von Quantum in den USA und/oder anderen Ländern.

Intel und Itanium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

SoftLayer ist eine eingetragene Marke von SoftLayer Inc., einem IBM Unternehmen.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Bedingungen für die Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit
Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung
Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung
Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens nicht vervielfältigen, weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Rechte
Abgesehen von den hier gewährten Berechtigungen werden keine weiteren

Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Verordnungen, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Dieses Softwareangebot verwendet keine Cookies oder andere Technologien zur Erfassung personenbezogener Daten.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und auf der Seite "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm-.com/software/info/product-privacy.

Glossar

Ein Glossar mit Begriffen und Definitionen für die IBM Spectrum Protect-Produktfamilie ist verfügbar.

Siehe das Glossar für IBM Spectrum Protect.

Glossare für andere IBM Produkte finden Sie unter IBM Terminologie.

Index

N

O

P

R

S

T

U

V

W

Z

Programmnummer: 5725-W98
5725-W99
5725-X15